Banking Services Operations

ISBN No.: 81-314-1037-4

Ref. No. BSO – 10200720

For any clarification regarding this book, please write to FedUni giving the reference number of the book, and the page number.

While every possible care has been taken in preparing the book, FedUni welcomes suggestions from students for improvement in future editions.

Banking Services Operations

Contents

Banking Services Operations

Detailed Curriculum

Introduction to Banking Operations: The Changing Nature of Banking Operations – Importance of Customer Relationship Management in Banks – Different Types of Products and Services Offered to Customers – Role of Technology in Banking Operations – Bookkeeping and Maintenance of Accounts – The Need for Asset-Liability Management – Regulatory Framework for Compliance.

Services Design and Delivery Strategies in Banks: Products and Services Offered by Banks – Designing of New Products and Services – Response of Banks with Newer Services and Delivery Mechanisms – Delivery Strategies in a Bank – Designing of Service Quality –Steps to Implement Delivery Strategies – Implications of Service Intangibility.

Introduction to Electronic Banking: Electronic Banking – Electronic Banking: Market Assessment – E-Banking: An Introduction – Internet: E-Commerce, E-Banking – E-Banking in India – Internet Banking Strategy – Risks in E-Banking.

Security Considerations in E-Banking: The Need for Security – Sources and Types of Risks – Causes of Risks – Control Measures at System Level and Network Level – Disaster Recovery and Contingency Plans – Legal Aspects and Framework – Security Policy.

Recent Trends of IT in Banking: The Branch Renaissance – The Migration to an Online Environment – Customer Relationship through Portals – The Digital Age of Banking.

Facilities Management: Cost Reduction Exercise – Role of Technology – Significance of Computerization in Banks – Finance Portals for the Banking Industry – Multi-channel Operations (Remote Banking) – The Regulatory Framework.

Payment and Settlement Systems: Payment Methods – Electronic Fund Transfers – Automatic Teller Machines – Electronic Clearing Service – Electronic Data Interchange – Financial Networks in India – Real-Time Gross Settlement Systems – Digital Certificates.

Payment and Settlement Systems, RTGS and Clearing House: Emerging New Instruments – Risk Factors for Payments Systems – International Standards on Payment Systems – Role and Concern of Central Bank and Participants – Payment and Settlement Systems in India –Real Time Gross Settlement – Developments in the Payment and Settlement Systems – Clearing House.

Service Quality Metrics: Core Factors – Customer Relationship Management – Technical Quality and Functional Quality – Role and Process Capability for Managing Services – Managing Service Delivery – ISO 9000 Certification in Banking Services.

Improving Quality and Productivity: Banking Services: Technical Quality and Functional Quality – Determining What Satisfies the Customer – Customers' Perception of Banking Service Quality – Devising Quantitative Determinants – Non-Quantitative Determinants – Quality by Design: Formulating a Suitable Standard – Quality Assurance – Improving Productivity and Performance.

Operational Controls: Banking Regulations and Supervision – Maintenance of Documents and Records – Adequate Information Storage and Retrieval Mechanism – Maintenance of CRAR – Reporting – Asset-Liability Management System – Organizational Structure – Audit and Vigilance.

Introduction to Risk Management: What Risk is All About – Basic Purpose of Risk Management in Banks – The Process of Risk Management – Different Types of Risks in Banks – Overview of Enterprise-wide Risk Management in Banks.

The New Basel Accord – Implication for Banks: An Overview – Basel II Framework – The Three Pillar Architecture – Organizations Affected by Basel II – Impact of Basel II.

Operational Risk Management: Operational Risk and its Evolution – Major Sources of Operational Risk –Measurement of Operational Risk – Management of Operational Risk.

Risk Management Strategies: Operational Risk Management Strategies – Financial Risk Management Strategies – Systemic Risk Management Strategies – Risk Limitation – IT Implementation Challenges.

Chapter I

Introduction to Banking Operations

After reading this chapter, you will be conversant with:

- The Changing Nature of Banking Operations
- Importance of Customer Relationship Management in Banks
- Different Types of Products and Services Offered to Customers
- Role of Technology in Banking Operations
- Bookkeeping and Maintenance of Accounts
- The Need for Asset-Liability Management
- Regulatory Framework for Compliance

Banking has flourished in India since the ancient times. The Rig Veda mentions indebtedness and some of the earliest dharma shastras lay down rates of interest and regulations governing debts and mortgages. Thus, a money economy existed in the ancient Vedic times. References to money lending for business purposes are found in the Manu Smriti too. The Jatakas of the Buddhist period, archeological discoveries and the literature relating to it, contain evidence of the existence of "Sreshthis" or bankers.

Early on, trade guilds acted as bankers both for receiving deposits and issuing loans. In South India, in particular, the larger temples served as bankers. The village communes occasionally advanced loans to peasants. In the process of emergence of systems for performing such banking operations during the early era, the Vaishyas emerged as a class of indigenous bankers and 'hundi' emerged as the earliest form of bill of exchange in India. These two developments can be considered as two important landmarks in the history of Indian banking. Indigenous bankers played a very important role in lending money for trade and commerce. Every town, big or small, had a Seth, a Shah, a Shroff or a Chettiar, who performed a number of banking functions.

Expansion of trade and commerce, both in terms of quantity and geography meant that the concept of banking would only gain more importance. Banking operations gradually transcended from individuals to groups and later on to companies. The Industrial Revolution of the 18th and 19th centuries, can be termed as an important landmark that helped widen the spread of banking operations. Banking is continuously and dramatically changing over the past few years. In a modern economy, banking plays an indispensable role. Banks today offer a wider range of products and services and deliver them faster and more efficiently than ever before. But the central function of banking still remains the same – mobilizing the savings (deposits and investments) of the economy towards investment.

While banking did not enjoy a steady and harmonious growth, it emerged and evolved through various phases adapting itself continuously to meet the increasing needs of trade and commerce.

The following 'core' areas have a bearing on the operations in the banking system.

- Changing nature of banking operations
- Different types of products and services offered to customers
- Role of technology in banking operations
- Importance of customer relationship management in banks
- Bookkeeping and maintenance of books of accounts
- The need for asset-liability management
- Regulatory framework for compliance.

CHANGING NATURE OF BANKING OPERATIONS

In India, the indigenous bankers played a very important role in lending money and financing foreign trade and commerce during the Moghul period. During the British rule, the agency houses carried on the banking business. The Hindustan Bank was the first bank to be established in 1779 followed by the General Bank of India in 1786. In the first half of the 19th century, the East India Company established three banks the Bank of Bengal in 1809, the Bank of Bombay in 1840 and the Bank of Madras in 1843, which were known as "Presidency Banks." These three banks were amalgamated in 1920 and a new bank, the Imperial Bank of India was established on 27th January, 1921. With the passing of the State Bank of India Act in 1955, the Imperial Bank of India was taken over by the newly constituted State Bank of India. The Reserve Bank, which acts as the Central Bank was created in 1935 with the passing of the Reserve Bank of India Act, 1934. The Swadeshi movement gave a fillip to the Indian joint stock banking and several of

the present leading public sector banks were established around this time as private banks. By 1913, there were 41 Indian banks in the field that included the Punjab National Bank Ltd., Bank of India Ltd., Canara Bank Ltd., Indian Bank Ltd., Bank of Baroda Ltd., Central Bank of India Ltd., etc.

Modern banking in India started at the end of the 18th century with the establishment of Bank of Calcutta in 1806. Bankers mostly from Scotland managed these new banks. Their practices and policies got ingrained into the Indian banking system. Basic accounting practices and the cash credit systems taught by the Scottish bankers are still in vogue in India.

The present day Indian banking system has three tiers. These are the scheduled commercial banks; the regional rural banks, which operate in rural areas, not covered by the scheduled banks; and the cooperative and special purpose rural banks.

There are approximately 80 scheduled commercial banks, both Indian and foreign; almost 200 regional rural banks; more than 350 central cooperative banks, 20 land development banks; and a number of primary agricultural credit societies. In terms of business, the public sector banks, namely the State Bank of India and the nationalized banks, dominate the banking sector.

Scheduled commercial banks constitute those banks, which have been included in the Second Schedule of the Reserve Bank of India (RBI) Act, 1934. These banks enjoy certain privileges such as free concessional remittance facilities and financial accommodation from the RBI. They are also obliged to maintain a minimum Cash Reserve Ratio (CRR) with the RBI. Some co-operative banks albeit not all are scheduled commercial banks.

The core banking operations include:

i. **Financial Transactions:** The bank will have the ability to pay bills and do transfers as part of the financial transactions handled by the system. The bank may choose to make available only some of these financial transactions based on business requirements. In some countries the financial institutions may be required to obtain regulatory approval.

ii. **Loan Origination/Application Processing:** The Internet banking initiative will provide a convenient interface for customers to apply for loans from their homes. Customers can look at the details of the available and the related facilities available.

iii. **Trade Finance:** The Trade Finance application offers the bank's corporate customers interactive access and connectivity through the Internet in a secure manner. It allows the bank to set-up a letter of credit application on its home page on the World Wide Web.

The present banking system can be classified as follows:

Public Sector Banks

- State Bank of India and its 7 associate banks called the State Bank Group
- 19 Nationalized Banks
- Regional Rural Banks sponsored by Public Sector Banks.

Private Sector Banks

- Old Generation Private Banks
- New Generation Private Banks
- Foreign Banks in India
- Scheduled Co-operative Banks
- Non-Scheduled Banks.

Co-operative Sector Banks

The co-operative banking sector was developed in the country to supplement the village money-lender. It comprises:

- Central Co-operative Banks
- State Co-operative Banks
- Primary Agricultural Credit Societies
- Land Development Banks
- Urban Co-operative Banks
- State Land Development Banks.

Development Banks

Development Banks are those financial institutions, which provide long-term capital for industries and agriculture, namely:

- Industrial Finance Corporation of India (IFCI)
- Industrial Development Bank of India (IDBI)
- Industrial Credit & Investment Corporation of India (ICICI)
- Industrial Investment Bank of India (IIBI)
- Small Industries Development Bank of India (SIDBI)
- National Bank for Agriculture & Rural Development (NABARD)
- Export-Import Bank of India
- National Housing Bank.

IMPORTANCE OF CUSTOMER RELATIONSHIP MANAGEMENT IN BANKS

Traditionally, banking was "personal" where the customer knew the bank employee and vice versa. By tracking the previous business done by the customer, the employee could anticipate his or her needs. The main bondage is the relationship the customer enjoys with the bank – the closer the customer feels to the bank, more are his or her chances of remaining as the "future customer".

But things have changed a lot over a period of time. We are now in a situation wherein newer technologies contribute to lack of personal touch and a customer can be lured by big financial institutions somewhere at the other end of the world by providing services better than any other local bank.

However, irrespective of the business strategy it decides to pursue, a commercial bank has to be customer centric in terms of products and services. More banks are turning to customer relationship management in search for more effective ways to woo and retain corporate clients.

Offering the right product to the right customer at the right time through the right delivery channel is the basic concept of CRM. CRM is driven by banks' realization that they can no longer expect to own their customers. While some are trying to own pieces of customer relationships, very few have the ability to deliver a comprehensive package of services under one umbrella. The primary goal is to uncover cross-selling opportunities and provide more customized services to retain customers. As a result, banks want a better understanding of how much of their customers' financial business they are actually handling and how many products they are selling to these customers.

In real terms, CRM can be implemented only if proper infrastructure is created. To implement this system, a bank needs to have an Apex Level Marketing and Business Intelligence function at the corporate level. Most of the banks today are

concentrating on publicizing their products and services and not concentrating on CRM. In CRM, a bank must know the value of customers. Therefore, the introduction of concepts like, Customer Profiling and Segmentation, Target Marketing, Wallet Share Analysis, Customers' Lifetime Value Analysis, Target Marketing, Campaign Analysis etc., become necessary. A bank will also be required to collect continuous feedback on the recall value and take necessary steps to improve the brand image. Unless a Business Intelligence system is set-up based on data warehouse or other repositories and a strong marketing team put in, it would be difficult to implement a CRM system.

Box 1: Banking on CRM

The volatility of global equity markets over the past few years has turned the tables on institutional finance firms in the capital markets, wealth management, and commercial banking sectors. Wealth management clients, tired of looking at dwindling account balances, are demanding from financial advisors long-term strategies to boost their assets. In the commercial banking sector, rock-bottom interest rates have made corporate lending a low-revenue business, prompting banks to look for additional noninterest-related income streams. In addition, consolidation in the market has increased the need for these firms to ensure as they build and retain close relationships with their most profitable customers – not only to prevent them from taking their business elsewhere, but also to ensure that they are offered the products and services that are the most appropriate and the most likely to result in new revenue for the bank.

Financial institutions are increasingly using customer management solutions with sophisticated front-office analytical capabilities that allow them to better slice and dice their customer data and use this insight to segment their clientele for better targeted selling opportunities. Gone are the days when each advisor alone had access to have individual schedules and client preferences and objectives. Today's investment firms and commercial banks need to employ a customer management solution that consolidates information from all customer interactions, whether they are in-person meetings with advisors or inquiries to the call center or the Internet. Moving forward, it will be imperative that every banking representative has the ability to access a 360-degree view of any customer in real time to enhance customer retention and competitive advantage.

Quick & Reilly, which offers financial services to more than 1 million clients as part of Fleet Boston Corp., has recognized measurable gains in productivity and competitive advantage thanks to a customer management platform that serves as the cornerstone of advisors' daily activities. The Quick & Reilly solution allows the investment firm to synchronize all customer information from first point of contact, and makes it available to all channels simultaneously. As a result, Quick & Reilly has experienced a dramatic increase in both employee productivity and customer retention. Additionally, its financial consultants have become more successful in the targeted cross-selling of products and services.

Initial successes like this have prompted new interests among financial institutions in using analytical information to drive targeted selling. The idea of cross-selling or up-selling existing customers is not new. For years, institutions have broadcast credit card offers, for example, the customers who fit in a specific minimum profile. Today's institutions, however, increasingly use analytics to determine which clients are more apt to sign up for a home equity line of credit instead – increasing not only the institution's top-line revenue, but also increasing wallet share and loyalty within the institution's existing customer base.

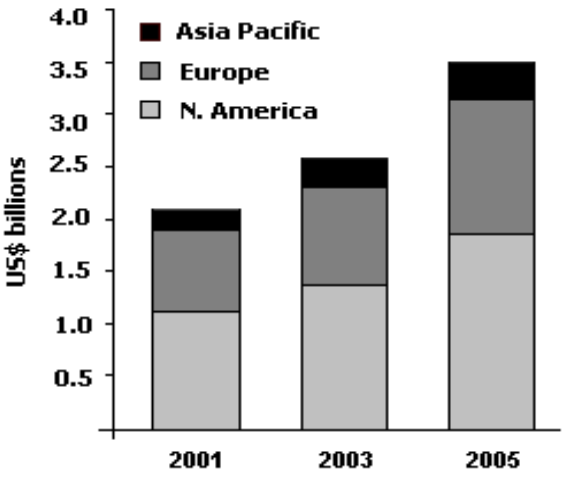
Analytical insight into customer relationships and activities also can provide institutions with a clearer picture of the profitability of specific customers to guide the level of service offered. Commercial banks looking to upsell recurring, fee-based cash management services to their lower income-generating lending customers can quickly determine which customers are not migrating to these other products and then offer differentiated service based on customer profitability to the commercial bank.

So, what lies ahead for financial institutions looking to maximize their customer relationships? Some forward-thinking institutions are beginning to turn their analytics systems inward, looking at their customer interactions to determine which advisors or products and services are doing well in specific branches or regions – and why – and then creating programs to replicate that success elsewhere. As markets begin to rebound, financial institutions that use analytical tools to ensure that targeted selling campaigns are presented to the appropriate prospects can ensure product and services adoption by customers and increase their revenue and profitability.

Source: www.destinationcrm.com/articles/default.asp?ArticleID = 4386

The trend of banks focusing upon re-engineering the existing services and introducing newer customer services gained momentum during the late nineties, close on the heels of globalization of the financial system. Thus, banks began to sell their customers online banking and consultation services to add both value to their services and to satisfy their customers. But even after selling a series of financial transactions to the customer on the Internet, the customer needs a good reason to remain loyal to the bank. Furthermore, at one end, the interaction between the bank and its customers has become less, and on the other, scores of financial institutions have burgeoned and are trespassing into the arena of banking. This includes introduction of new channels via newer technologies like Internet Banking, ATM, Phone Banking, and VRU (Voice Response Unit). As use of the Internet continues to expand, more banks are using the Web to offer products and services or otherwise enhance communication with consumers. But once a customer is online, it is hard to keep him or her loyal to the bank. The following graph shows the amount of spending by banks in CRM across various regions.

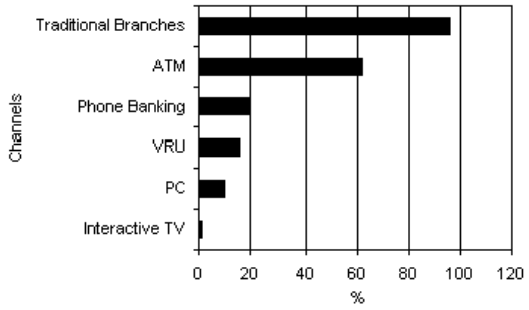
Figure 1: CRM Spending by Region



Source: Celent Communications.

Of late, banks have realized that successful migration of customers to the Internet lies in transferring the offline relationship to online environment.

Figure 2: Percentage Use of New Channels Offered by Banks



Source: Boston Consulting Group.

According to the Tower Group, a research and advisory firm, banks and other financial institutions are certainly not new to the technology having spent $5.1 billion on CRM in 1999. But the retail-oriented banks aiming to retain individual consumers spent 78 percent of that money.

For instance, Fleet Boston Financial unveiled plans to use the technology of business and CRM software supplier Micro Strategy earlier in 2002 as the basis for a Web portal run by its Corporate and Global Banking Business Group. Fleet Boston, US's eighth largest diversified financial services company with $181 billion in assets, will leverage the technology to let CRM specialists at the bank view a corporate or institutional client's transaction history. This type of review should enable a manager to better manage the client's contacts with the bank. Financial analysts will also use the technology to segment customers in product usage categories and to spot imbalances in client investment, debt, equity and capital structures.

A significant improvement in customer relationship can be achieved when the technology provides the customer information, which he/she wants, the place, time and how he/she gets it. This would not only make him/her feel close to the bank but also enhance the bank-customer relationship. Only when the customer feels valued, will he/she reciprocate the relationship with loyalty. This bridges the gap and provides a virtual interpersonal connection – "an exceptional customer service".

For this, the bank might need to bring about a change in the existing business models. It can be accomplished in the following ways:

i. Dividing its customers in various categories like Retail, Small and Medium Enterprises and Corporates and further subcategorizing them for increasing the overall focus on customers. Or a bank simply can categorize its business into two parts – Retail and Corporate.

ii. The bank can categorize its customers in segments like Personal Finance, Business Finance, and Corporate etc. Banks can also add additional lines of business considering businesses on which they would like to focus.

iii. A bank may also decide to follow a niche strategy. Some private sector banks indicate that they would concentrate solely on corporate sector. Some of the foreign banks may decide to set-up NBFCs to exclusively focus on niche areas by taking on activities like commercial investments, business and management consultancy, leasing and financing.

iv. A bank can adopt "Universal Banking". One of the large public sector banks is in the process of transforming itself into a universal bank and all its branches accordingly are getting converted into financial supermarkets capable of dispensing all services and products including insurance.

The objective of segmented business model approach is to have a sharper focus on the customers and on providing the best service possible. While formulating such business model, a bank has to take into account two major aspects:

i. The Business model needs to have flexibility and adaptability so that in case of any future change in focus, there will not be a need to start from the scratch.

ii. A bank, while adopting a business strategy, should not lose focus of its perceived future growth path. One of the major issues for consideration would be the path of growth it would wish to pursue. If a bank decides to grow using the inorganic route, its business model should have lot of flexibility to incorporate a new business.

Box 2: The Customer's Voice: A Powerful Boost for CRM Effectiveness

Failure to consider customer feedback limits the effectiveness of CRM, according to a report from Customer Relationship Metrics.

"Many of these initiatives come from top-level executives, who are usually far removed from customer interaction," says Jodie Monger, Customer Relationship Metrics president, who authored the report with Cherie Keen, the company's vice-president of research and client services. "Although companies may have initiated several solutions that are supposed to improve customer satisfaction, many are flawed because of (the company's) neglect in bringing the customer into the mix."

Though companies attempt to evaluate the effectiveness of their CRM programs based on benchmark data, these evaluation methods tend to ignore the customer's opinion. "When all is said and done, it's the customer that has the final say if you have the best practices," the report states. Neglecting the voice of the customer limits, the effectiveness of programs designed to improve customer satisfaction.

Companies that can link caller evaluations to the agent can improve first-contact resolution and focus training and coaching on the agents who need it most. Increased first-contact resolution percentages yield higher contact satisfaction and contribute directly to customer loyalty, according to the report.

Customer Relationship Metrics tested this theory in two contact centers over a six-month period. Each one began a voice-of-the-customer program to collect feedback through a post-call customer survey. Each call center implemented the program differently.

For example, Contact Center A, using a completely automated recording system, collected results linked to the specific agent who handled the call and could record verbal comments from customers. In doing so, Contact Center A increased first call resolution by 10.3 percent, resulting in 3,120 less repeat calls per month. The result was an annual cost savings of $187,000 (based on $5 per call and 30,000 calls per month).

On the other hand, Contact Center B collected total results, rather than results tying specific calls to specific agents. Verbal comments were not recorded. Contact Center B saw a 2.9 percent decrease of first-contact call resolution, which translated to an additional 870 repeat calls per month and $52,300 in increased annual expenses.

"Quality is important, because in today's commoditized economy, the only differentiating factor and competitive advantage a company has is the service it provides," Monger says. "All too often companies that have the best product become extinct due to poor customer service." The report recommends that call centers use completely automated telephone surveys that enable randomly selected customers to take a satisfaction survey immediately after a call, as Contact Center A did in the study, because such a system not only reduces calls, but also provides a higher return on investment for training and coaching.

Some call center managers have implemented a monitoring program that involves 5 to 20 live and remote monitoring sessions each month. The problem with this type of system, according to the report, is that it doesn't take into account the different methods needed to handle different customer calls efficiently and effectively. "A monitoring form should be a dynamic instrument that can handle different types of interactions with the ultimate goal being "The customer was satisfied and a repeat contact on this issue should not occur," Monger says.

Therefore, the measurement system must be in step with the customer's preferred communication channel. This isn't the case when a customer phones in and the company follows up with an e-mail survey, or if the customer e-mails a company, which then follows up with a phone survey. "To best measure the effectiveness of service delivery an immediate evaluation is needed via your customer's preferred channel," Monger says. "This will ensure the success of your voice-of-the-customer program, (and) increase your customers' satisfaction and loyalty. It creates the ideal situation that contact center managers are searching for."

Source: http://www.destinationcrm.com/articles/default.asp?ArticleID=4439

DIFFERENT TYPES OF PRODUCTS AND SERVICES OFFERED TO CUSTOMERS

We also find that just as in the case of CRM, the product-needs and product-preferences of customers also undergo changes. Therefore, even to effectively implement customer segmentation based business model, it is necessary to refine the products and services. In this regard, it is not just sufficient to introduce cosmetic changes in the existing products and services to retrofit in various business segments. Thus, banks should clearly perceive the requirements of customers and come out with segment specific-products and services.

For introducing new products and services or pulling out obsolete ones from the market, it is necessary to have a proper system of business intelligence. This requires monitoring the competitors' moves on products and services front including quality and prices and introduction of new products and services for which it would be worth emulating foreign banks. By setting up a formalized system of receiving continuous feedback from customers, it will be possible for the banks to develop a highly innovative product or service capable of creating a better brand for itself.

Growing expectations of the customers drive business strategies for the banks, thereby causing changes in the banks' operations. In line with the maturation trend in banking industry, the thrust of business strategy has been shifting from what is termed as 'Product based' to 'Customer focused' approach. Customer centricity has already become the focal point in banking operations.

Switching over from plain products and services to offering tailor-made products to individual customers, advisory services, availability of preferred delivery channels, walking ATMs and OSAs on constant move to deliver banking services at doorsteps, bundled products and services offer, market risk mitigating products, demonstrates how the banks have been fine-tuning their business strategies towards achieving customer centricity and convenience.

Most of the above mentioned products and operations are technology-based and do not involve a human touch in operations. Nevertheless, the importance of human touch in operations is evidenced by the fact that steps to improve branch operations are also being simultaneously carried out.

Branches are the basic delivery channels of products and services. Hence, the counter services at the branches should be fine-tuned in relation to customer centric business model. Under any technology-enabled transformation, branches are required to focus on sales and services. This is possible only if all the back

office functions from branches could be taken away and put at a central place. In this context, the system of regional processing center, and centralized system of loan processing become extremely important. Functioning of Universal tellers and relationship managers at the grass roots level can help in setting up a customer centric model. The basic rule is that all the banking requirements of the customers should be taken care of by the tellers. In a highly technological environment, a customer of any line of business/branch should be able to get the banking service at any branch. At present, not many banks are equipped to provide such levels of service. But for driving a customer centric business strategy such changes in the branch functioning would definitely be required. Banks are opening branches despite having highly developed internet and mobile banking systems. But the shape and ambience of branches are bound to change in the light of technology enabled business transformation of banks. Easy identification of a branch with its sleek ambience and large area of the branches for customers rather than for the bank staff will be a common feature. A hypothetical view on the workflow of a customer entering in such branch can be as follows:

i. A customer entering in the branch is welcomed by a Customer Relationship Manager and is directed to a counter where his banking related requirements are to be met.

ii. The branch is fully equipped with online ATMs which help him withdraw cash and fulfill other related requirements.

iii. On the Internet kiosk, he can find out about new products, apply for loans, make online payments, get other internet-based information etc.

iv. From a set of neatly stacked section-wise brochures he can get all minute details about various products and services.

v. If customer is a global investor he can find details about the growth of the funds invested (corpus) and the future outlook.

vi. A host of financial research material providing latest developments and current and future outlook are available in the branch for the customers' use.

vii. If it is a corporate finance branch and the customer a high net worth person, financial analyst can assist him in business needs and provide all advisory services.

ROLE OF TECHNOLOGY IN BANKING OPERATIONS

The availability of technologies like enterprise level core banking solution is proving a great enabler to run any business strategy covering all business units operating under a fully automated and networked business environment. Networking and internet-based technologies, besides enabling banks to handle large volumes of businesses in an orderly manner, have also helped provide many advantages such as demolish physical boundaries for delivering cross-border services, enabling the customer to avail major banking services from any corner. Networking and usage of internet-based solutions has made it possible for any customer to view his/her accounts details, undertake fund transfers and comply with standing instructions.

Continuous fall in the price of hardware and networking cost and increased bandwidth will only accelerate the pace of such advancement, enabling the banks to reduce the cost of transactions and overheads. Fully integrated systems enable banks to have a single version of truth. Providing the customer with a choice of delivery channels also becomes easy. Payment gateways will bring about a new era in payments, promote customer centricity, accelerate the pace of funds transfer on the real time basis and bring about a new way of functioning of the banking industry.

From the point of view of improving spread and profitability, it is necessary for the banks to reduce the cost of a transaction. Technology obviously plays a key role in serving this objective. The biggest advantage of having a strong technological solution lies in enabling a bank to handle volumes of services in a seamless manner. A bank, even with the minimum spread, can become a highly profitable bank through handling large volume of business using technology. Another issue is service dispensations through delivery channels – the cost of handling banking transaction is minimum on internet and maximum in a branch. Thus in a bid to maximize profitability, customer convenience and transaction costs, a bank will have to adopt a strategy where it can motivate its customers to avail their banking facilities on a suitable delivery channel.

Business Process Re-engineering (BPR) and Business Process Outsourcing (BPO) are two other areas on which focused attention need to be made to take full advantage of business transformations. With a proper system of BPO and BPR coupled with technology, a bank can reduce the cost of operations/transaction to maximize its profitability.

The general expectations are that the banking sector should do well for the next 2/3 years due to the proposed changes in the banking industry by the regulators. The asset recovery norms will pave the path for majority of the banks in recovering their bad debts and provide an impetus to the bottom lines of their balance sheets. Banks are focusing on improving the service standards by incorporating latest technology and reducing the costs overhead. The banking industry is also in an overdrive to cut cost and improve service standards by merging networks and switches, sharing ATMs and forming alliances for mutual benefits. The boom in the retail sector lending has created opportunities for banks to push forward their growth aggressively in this segment. The growth in the Indian economy today presents ample opportunity for banks to expand their business and increase their overall profitability.

BOOKKEEPING AND MAINTENANCE OF ACCOUNTS

In simple words, ‘accounting’ means ‘reckoning’ or ‘recounting’. In an organizational context too accounting carries more or less the same meaning. The process of accounting includes recording, classifying and summarizing of past events and transactions of financial nature, with a view to enable the user of accounts to interpret the resulting summary. The utility of accounting information is greatly increased when it is compiled in a systematic manner and financial statements are prepared at periodic intervals. For the purpose of compilation, all monetary events are recognized as transactions and classified into various account heads. The account heads are then summarized under related and significant groups so that interpretation becomes possible. One must also understand the difference between accounting and bookkeeping. Accounting is broader in scope than bookkeeping, which is merely concerned with orderly record keeping. Going beyond the narrow confines of bookkeeping, accounting involves analysis and judgment at different stages such as recording of transactions, classification, summarization and interpretation.

The bookkeeping system of a bank is different from that of a company or an industry. Since banks have to deal with a lot of customers for various transactions, a large number of books of accounts is maintained. To avoid any kind of mistakes in the books of accounts of customers, the accounts are checked on a daily basis. Some of the characteristics of a bank’s bookkeeping system are as follows:

i. Most of the banks maintain subsidiary books as, personal ledgers and bill registers. Bill registers are kept in separate registers. Examples of bills registers are bills purchases, inward bills, outward bills for collection etc. Entry is made on a day-to-day basis. Separate ledger forms are maintained for bills purchased and discounted. Personal ledgers are kept in ledgers. They may be cash certificates, current accounts, fixed deposits, etc.

ii. Other subsidiary registers maintained by banks include, Registers for Demand Drafts, Telegraphic Transfers and Mail Transfers issued on/received from branches and agencies and Letters of Credit and Guarantee.

iii. While the above mentioned are the general ledgers and books maintained by the banks, there are also certain departmental journals which are maintained by each of the department of a bank to keep track of the transfer entries passed by it. These journals are memoranda of books only, and all the entries made in these books are also made in the Daybook through Voucher Summary Sheets. The purpose of these books is to maintain a record of all the transfer entries from every department. For example, the loan and the overdraft section will pass transfer entries for interest charged on various accounts every month, and all these entries will be posted in the journal of that department. The concerned office can easily find out the accounts in respect of which the interest entry has been passed. Since all the vouchers passed during the day are entered into the Daybook only in a summary form, it may not be possible to get this information from the Daybook without looking into the individual vouchers. Added to this, since the number of departments in a bank is quite large, the Daybook may not be accessible at all times to all departments.

iv. The various departments of the bank also maintain certain books. These are the memoranda books that facilitate their work. Some of the important memoranda books in the cash department are:

   a. Receiving Cashier's Cash Book

   b. Paying Cashier's Cash Book

   c. Main Cash Book

   d. Cash Balance Book.

The main cash book is maintained by persons other than the cashiers. Each cashier keeps a separate cash book. When cash is received it is accompanied by pay-in-slip. The cashier makes the entry in his book, which is checked by the chief cashier. The pay-in-slip then goes to the main cash book writer who makes an entry in his books. The cash book checker checks the entry with the slip and then the counter-foil of the slip is returned back to the customer and the foil is sent to the appropriate department for entering into the ledger. The foil is used as a voucher. Cheques, demand drafts, pay orders, etc., are themselves used as vouchers.

i. **Quick Payment System:** Banks introduce different systems to facilitate quicker deployment of services. The most prevalent system is the teller system in which the teller keeps cash, ledger cards and the specimen signature cards for each customer. He is authorized to make payment up to a particular amount. On receiving cheque, he checks it and passes it over for payment. He then enters it in the ledger card and makes the payment to the bearer. He also accepts cash to be deposited into accounts.

ii. **Onward Clearing:** The onward clearing book is a clearing "cheque received" book for entering cheques received and a bank-wise list of the above cheques. A copy of the onward clearing books is sent to the Clearing House along with the cheques. A person checks the vouchers and lists with the "clearing cheque received" book. These vouchers are then sent to appropriate departments, where customers' accounts are immediately credited. If any cheque is returned unpaid, the entry is reversed. In the usual practice, no drawings are allowed against clearing cheques deposited on the same day, but the manager in the case of established customers makes exceptions.

iii. **Inward Clearing:** Inward clearing relates to the cheques that come into the bank. Cheques received are checked against lists. They are then distributed to different departments and the number of cheques given to each department is noted in a Memo book. When the cheques are passed and posted into ledgers,

their number, once again is tallied with the Memo book. If any cheques are unpaid they are then returned to the clearing house. Here it must be noted that the cheques themselves serve as vouchers.

iv. **Loans and Overdraft Departments:** The following books are maintained in the loans and overdrafts departments:

a. Registers for shares and other securities held on behalf of each customer.

b. Summary books of securities giving details of government securities, shares of individual companies etc.

c. Go-down registers maintained by the go-down keeper of the bank.

d. Price register giving the wholesale price of the commodities pledged with the bank.

e. Overdraft sanction register.

f. Drawing power book.

g. Delivery order books.

h. Storage books.

- **Deposits Department**
  a. Account opening and closing registers.
  b. For fixed deposits, rate register giving analysis of deposits according to rates.
  c. Due date diary.
  d. Specimen signature book.
- **Establishment Department**
  a. Salary and allied registers such as attendance register, leave register, overtime register, etc.
  b. Register of fixed assets, for example, furniture and fixtures, motor cars, vehicles, etc.
  c. Stationary registers.
  d. Old records register.
- **General**
  a. Signature registers.
  b. Private telegraphic code and cyphers.

THE NEED FOR ASSET-LIABILITY MANAGEMENT

The Indian financial sector reforms in the 1990s brought unprecedented changes in the banking sector. The interest rates deregulation, the opening up of the various financial markets combined with the intensifying competition has been affecting the spreads of the banks. And, while these measures were initiated several years ago the adjustment process of the banks to these developments has not been satisfactory.

The pressures arising on the profitability, liquidity and sustainability of the bank cannot always be tackled on a firefighting basis. Such an approach may be successful in certain instances, but not at all times. A better alternative for the banks will be to take a strategic perspective while addressing the aspects related to the interest rate/exchange rate fluctuations, liquidity positioning, credit accommodation, etc.

To take a strategic perspective, banks should first of all understand the risks that have to be taken in order to gain the rewards that are set as the target. Banks are exposed to various types of risks and have a few risk management models at their disposal. This, however, leaves unanswered the question of how to implement the risk management process. The implementation part of the ALM, occupies a predominant position at the various levels of management.

Generally, implementation of ALM will involve strategic decisions which have to be developed internally by the bank's management. However, this has not been the case with most of the Indian banks. Though, the reasons for such lack of initiative are varied, one important reason could be that the Indian banks had so far been restricted to a closed operational environment with little exposure to the open market. Be that as it may, the lack of initiative by the banks towards ALM, in spite of its relevance, has forced RBI to step in and start off the process. As a regulator of the banking sector in India, RBI has developed an ALM framework. This framework discusses an ALM model based on Gap Analysis and is intended to introduce the banks to the process of ALM.

Based on the RBI model, banks can segregate their assets and liabilities into various maturity buckets and also identify those assets and liabilities, which are sensitive to interest rate movements. While deciding about the liquidity requirements in certain cases, the RBI has given only a benchmark. If adequate information is available to the ALCO of a bank on the maturity patterns of their assets and liabilities, it can set the liquidity limits for the different time buckets. Consider the case of current and savings deposits. Based on the previous experience, each bank can estimate the volatile and core portion of the current/savings bank deposit and hence can assess the liquidity requirements accordingly. The ratio of stable to volatile deposits is computed based on the consolidated figure of the savings bank/current deposit. Similarly, if the ALCO is able to forecast the movements of the interest rates with greater accuracy, using more sophisticated methods, it will then be in a position to ascertain the sensitivity of its assets and liabilities and take measures to prevent any adverse impact on its NIM and MV of equity.

There are a few issues that need to be raised in the RBI's classification of the assets and liabilities based on liquidity and sensitivity. In the case of export refinance, for instance, the RBI has mentioned that the maturity profile of the availed portion of export refinance has to be based on the underlying assets. This implies that there should be a case-to-case analysis to determine the maturity profile, which will be a tedious task. Instead, the bank can use the consolidated figure of the refinance (as in the case of the savings bank deposit account) and based on past experience can identify a core portion and a variable portion. The core portion can be classified under the 1-3 years bucket while the variable portion can be classified under 1-14 days time bucket. This can be a dynamic process if the distinction between core portion and variable portion are reviewed monthly. The core portion of the savings bank deposit is classified as sensitive and placed under the 3-6 months bucket. However, the frequency with which the savings bank rate changes is very low. In fact, the revision of savings bank rate along with revision in term deposit rates is more an exception than rule. Due to this reason, the core portion of the savings bank deposits may also be considered as non-rate sensitive. Further, the borrowings from the RBI are placed under the one-month time bucket for rate sensitivity purpose. The point to be noted here is that the borrowings are eligible for a period of 14 days which may be extended later. Thus, the time bucket for such borrowings may be 14 days instead of one month. However, the adverse impact of this may not be significant, since the rate change in this case will be brought about by the regulator and not by the market.

Banks can initiate the process of ALM using its framework given by the RBI. However, considering that the framework is developed for the common use of all banks, there will be a definite scope for banks to develop this model based on the operational styles and the information systems available to them. Apart from this model, which targets the interest rate risk and liquidity risk of banks, the regulator has also been addressing the credit risk of the banks. The second set of guidelines on risk management relates to an integrated risk management system covering aspects related to credit risk, liquidity risk, etc. The RBI has also hinted moving

towards VAR and Duration Analysis. Even global regulations governing the credit risk given in the Basle Accord are taken into consideration. The various guidelines issued by the regulator are to ensure that the process of risk management becomes a regular exercise of the banking business. However, it has to be understood that the process of ALM is multifaceted and will vary from one bank to another. Banks should keep in view their requirements for managing the risks and do the needful for the successful implementation of the ALM.

REGULATORY FRAMEWORK FOR COMPLIANCE

The level of a country's economic development and its progress to a large extent is determined by the stage of development of its financial system. It is not just sheer coincidence to find that countries that have achieved higher levels of economic development find themselves placed around a better financial system and financial institutions as compared to less developed countries. A financial system comprises of a variety of complex institutions and people such as market regulations, laws, practices, money managers, analysts, transactions and claims and liabilities.

A financial system serves to fulfill the capital needs of businesses. The capital is made available to the business sector after the funds are sourced from people who have surplus money. Capital can be needed either for a short-term between one day and one year or for a longer term of more than one year. The source for short-term finances is the money market while the long-term finances are raised from the capital markets. Incidentally, the money market instruments have shorter maturity periods as against the capital market instruments, which have longer periods of maturity. Both the above types of markets use public money augmenting the need for an organization, which could oversee their functioning. In effect, the RBI and SEBI have been vested with the responsibility of developing the required regulations and monitoring the functioning of both the markets. The Reserve Bank of India is focused on framing policies for the development of the money market while SEBI is focused on framing policies for the development of the capital markets. As the functioning of the money market affects the capital markets and vice versa, these two regulatory bodies exist to complement each other in providing stability and growth to the financial system.

Within the financial system, banks play a key role since they are the major players in mobilizing savings and turning them into investments. The banking system can survive and grow only under an authority that can guide and monitor it. Thus, RBI emerged on the Indian banking horizon. Significantly, during the nineties, the emerging trend towards globalization aided by massive funds flow, contributed to the East Asian Crisis affecting several East Asian countries. Developments such as these only undermine the importance of the role played by the Central Bank of a country. In this context, the RBI is bound to be more responsible.

Box 3: Trends in Banking Sector

It's not the first time the Reserve Bank of India (RBI) has sent out early warning signals to the Public Sector Banks (PSBs). And it certainly isn't going to be the last. The latest RBI Report on Trend and Progress of Banking in India 2002-03 is particularly significant because it marks the completion of 10 years of banking sector reform in India. And taking off from that, RBI's report dwells on several aspects — positive and negative — of the Indian banking sector, issuing warnings wherever required.

If, after 10 years of reform, the PSBs are yet to read the writing on the wall, it is a reflection of the fact that having been sheltered for years, they are still taking time to understand the nuances of the new age. The clear signal which the RBI, under the stewardship of Governor Yaga Venugopal Reddy, now seeks to give PSBs is that the time has come for them to shake off the lethargy of the past and get their act together, or face the consequences of competition which a decade of reform has brought about.

RBI says in the report that its analysis clearly shows that much of the increase in profits of scheduled commercial banks in India has come about thanks to trading profits, fallout of the continuing decline in interest rates. But this is not banking as we understand it. And therefore, profits which aren't happening on account of the banks' core activity of lending need to be viewed with caution.

"It is in this context that the Reserve Bank has been emphasizing that high profitability emerging from gilt trading should not lull banks into a state of complacency," argues the RBI in its report. To the extent that the state-run banks' stock market performance is a result of this growth in profits, the profits from gilts trading and the rise in the banks' stock prices are also inextricably linked. And while this is a reality in today's context, the central bank in its report has clearly shot off the required warning. If banks did not lend during times of downturn and avoided what RBI calls "problems of adverse selection", then equally they need to recognize that while partaking of the benefits of a low interest regime through trading profits is all right, a bank's primary job is to lend, and support industrial activity and growth. This is what RBI advises the banks to get back to doing.

Pointing to the fact that trading profits have helped banks to shore up their bottom lines and provide for Non-Performing Assets (NPAs), RBI reminds them that the "primary business of banking is the creation of credit." Also, while the banks are enjoying the fruits of the lower interest regime on the trading front, the linkage between the debt and equity markets (with stock prices rising on expectation of trading profits by banks) also means banks have to take greater care in managing interest rate risks.

The good news, of course, is that a combination of factors has led to a significant decline in NPA levels. From as much as 15.7 percent at end-March 1997, gross NPAs have declined to 8.8 percent as at end-March 2003, through a combination of upgradations, recoveries and write-offs. This is now being added by the SARFAESI Act, popularly known as the Securitization Act, which has errant borrowers getting back to the negotiating table with banks.

But while things are looking better in general, and the return of the feel-good factor may spell better days for PSBs, the key issue for them is how they would now face competition from the aggressive, new generation private and foreign banks. RBI, as regulator, is acutely aware of this challenge, and has done its best to prepare the state-run banks on this front. The private and foreign banks are positioning themselves, the RBI report says, as one-stop shops for financial services. Against such a background, PSBs would need to look beyond just their traditional avenues of income and go into non-fund based, value added services to augment their non-interest incomes. That would also require better technology and a change in mindset. Simply put, PSBs have to get nimble-footed and creative if they have to win the race in the new banking era.

Source: http://www.financialexpress.com/columnists/full_column.php?content_id=46508.

As the banking regulator, the Reserve Bank of India has to monitor and regulate the risk taken by banks. Banking is a risky business as the recent developments involving the Global Trust Bank (GTB) indicate so clearly. The equity held by banks is very low, compared to the portfolio they build. If equity is 5 percent of total assets – the loans and bonds held by the bank – then a few loans going bad can lead to bankruptcy. And, this may not happen because of incompetence or corruption. It may be the ill-effect of the business cycle.

Yet, there is a stream of thought that believes that the way banking has been treated in India, gives an impression that banks have low-risk. People have been led to believe that money in banks is safe. The main reason has been the large share of public sector banks in India, which, even when managed badly, have not been allowed to go under. The response of the banking regulator to poor performance of banks has indeed been very mild. The RBI has not flexed its

muscles as the regulator and imposed penalties or ordered shutdown. Even when banks have violated existing regulations, such as capital adequacy requirements, it has not taken stern action. Worse, when things have gone bad, banks have been bailed out, been merged with other banks or given loans by the government. The capital injection of Rs.9,000 crore into IDBI in Budget '04 is an example of the phenomenon. This pattern of behavior by the government and the RBI has given wrong signals. If the regulator continues to act soft and does not take punitive action, the managements will come to believe that incompetence far from being punished would be rewarded. This could prevent improvement in the quality of management of banks.

Similarly, depositors should clearly understand that only balances of up to Rs.1 lakh are covered by deposit insurance. If depositors place more than Rs.1 lakh in a bank, they are taking upon themselves the credit risk of the bank. By bailing out public sector banks, every time there is a crisis, the RBI is creating the impression that no such bank will ever be allowed to go bankrupt. Unless banking regulation is strict, and weak banks are forced to shutdown, the health of the banking sector in the long-term cannot be ensured. The GTB crisis may have been overcome through its amalgamation with Oriental Bank of Commerce. However, the problem of weak regulatory compliance and the wrong signals it sends to depositors, does not get addressed. Therefore, the GTB crisis should serve as a much-needed reality check.

As the apex institution, the Reserve Bank of India plays the dominant role in developing the financial system. It lays down the policies to achieve an orderly growth of the financial system. In this process, the regulations are laid down covering the financial, government securities and the forex markets. We take a look at the policy framework of the Reserve Bank of India under these different markets and cover the contents under Organizational Framework and Operational Framework. The different departments of the Reserve Bank of India perform various functions as:

- **Department of Banking Operations and Development:** It is responsible for regulating commercial banks under the regulatory provisions of the Banking Regulation Act, 1949 and the Reserve Bank of India Act, 1934 and other relevant provisions in various statutes. Further, it plays the leading role in the development of banking policies. The department works towards fulfilling the objectives of promotion and development of a sound and competitive banking system. This is sought to be achieved by focusing on regulations concerning different areas such as prudential regulations relating to capital adequacy, income recognition, asset classification, provisioning for loan and other losses, investment valuation, accounting and disclosure standards, asset-liability management and risk management systems. Other important activities of the department include licensing of new banks, expansion of foreign and domestic banks, approval for setting up of subsidiaries and undertaking new activities by commercial banks and follow-up for rehabilitation of weak banks.
- **Department of Government and Bank Accounts:** It performs important central banking functions like acting as the banker to the Government and other commercial banks besides managing public debt of both, central and state governments. It also maintains the Reserve Bank's internal accounts and compiles its weekly and annual accounts. Other functions involve general banking business including management of public debt of the central and state governments devolved by virtue of the provisions of the Reserve Bank of India Act, 1934 in addition to the agreements entered into with the

respective governments. The above functions are carried out on a day-to-day basis through the Reserve Bank's official machinery consisting of Public Accounts Departments, Deposit Accounts Department, Public Debt Offices and the agency bank branches.

- **Department of Banking Supervision:** It inspects and supervises commercial banks in accordance with the provisions of the Banking Regulation Act, 1949. The function includes on-site inspection and off-site surveillance. This department is further divided into Department of Banking Supervision and Department of Non-Banking Supervision.
- **The Department of Currency Management:** It is responsible for administering the functions of currency management, which is an important function of the Reserve Bank in terms of the Reserve Bank of India Act, 1934. As part of this function, the RBI issues notes and coins and retrieves unfit notes from circulation through its 18 issue offices and a wide network consisting of 4195 currency chests, 488 repositories and 3562 small coin depots managed by banks and government treasuries.
- **The Urban Banks Department:** It is vested with the responsibility of regulating and supervising primary (urban) cooperative banks, which are popularly known as Urban Cooperative Banks (UCBs). It performs three major functions: regulatory, supervisory and developmental through RBI's 16 regional offices.
- **The Rural Planning and Credit Department:** It formulates policies relating to rural credit and monitors timely and adequate flow of credit to the rural population for agricultural activities and rural employment programs. It also formulates policies concerning the priority sector, which includes agriculture, small-scale industries, tiny and village industries, artisans and retail traders, professional and self-employed persons, state sponsored organizations for scheduled castes and scheduled tribes and government sponsored credit-linked programs.

Just as the promotional role is important, so is the regulatory role of the RBI. It is an essential role because the RBI has to control the overall credit and the price levels in the economy. It has to maintain the value of the rupee, ensure a sound and healthy banking system, and ensure effective coordination and control over the credit portfolio through appropriate monetary and credit policies reviewed from time to time. For achieving these objectives, it becomes essential to remove various imperfections in the financial markets and ensure accountability in the operations of various financial players.

Banking in India Today

The banking sector has undergone a massive restructuring during recent years as a result of recent developments. New technologies have added to the competition. The IT revolution has made it possible to provide ease and flexibility in operations to customers thus making banking simpler and easier. Rapid strides in information technology have, in fact, redefined the role and structure of banking in India. Further, due to exposure to global trends after the Information explosion led by Internet, customers – both individuals and corporates – are now demanding better services with more products from their banks. The financial market has turned into a buyer's market. Banks are also coping and adapting with time and are trying to become one-stop financial supermarkets. The market focus is shifting from mass banking products to class banking with the introduction of value added and customized products. Public Sector Banks like SBI have also started focusing on this area. SBI plans to open 100 new branches called Personal Banking Branches

(PBB) this year. The PBBs will also market SBI's entire spectrum of loan products, for example, housing loans, car loans, personal loans, consumer durable loans, education loans, loans against shares and financing against gold.

SUMMARY

- Banking operations have witnessed tremendous changes over a period of time due to the advancement in the technology or globalization or both. They have become far more advanced when compared to the past.
- One of the key challenges that banks face today is their ability to offer fee based services that can reach out directly to where their customers are and be profitable at the same time.
- Traditional banks have long been exposed to strong external pressures. These pressures include technological revolution, securitization, rising competition, deregulation, etc.
- There are two models emerging in the banking sector today. One of them is universal banking in which banks are attempting to provide products and services developed by them to customers. The second one is CRM.

Chapter II

Services Design and Delivery Strategies in Banks

After reading this chapter, you will be conversant with:

- Products and Services Offered by Banks
- Designing of New Products and Services
- Response of Banks with Newer Services and Delivery Mechanisms
- Delivery Strategies in a Bank
- Designing of Service Quality
- Steps to Implement Delivery Strategies
- Implications of Service Intangibility

The evolution of different products and services has been significant ever since the liberalization and financial sector reforms were ushered in the 1990s. Consequently, a major impetus has been given to the types of products, services and the manner of their delivery by the banks. The major influence of deregulation on the banking sector has been to make them open to competition and thereby make them more competitive. The entry of new private and foreign banks has brought in major changes in this regard. Undoubtedly, IT initiatives have made the banking operations easy and flexible to customers. Rapid strides in technology have, in fact, redefined the role and structure of banking. Further, due to exposure to global trends led by Internet, customers – both individuals and corporate – are now demanding better services with more products from their banks. Financial markets have turned into buyers' markets. Banks are also changing with time and are trying to become one-stop financial supermarkets. Market focus is shifting from mass banking products to class banking with introduction of value added and customized products.

In this chapter, we shall initially focus on the various products and services offered by the banks. Then, the focus shifts to the various factors that influence the design and delivery of products and services. In this regard, we try to understand the response of the banks to such requirements and thereby underline the importance of redesigning delivery strategies in meeting the customers' needs.

PRODUCTS AND SERVICES OFFERED BY BANKS

We now discuss some of the products and services offered by banks customers and which have been specially designed taking into account the requirements of customers from time to time.

Installment Credit

Installment loans require the periodic payment of principal and interest. In most of the cases, the customers borrow money to buy durable goods or cover extraordinary expenses and the loan is to be repaid in installments[1]. The typical maturity ranges from two to five years. Except revolving credit, most consumer loans are secured. Installment loans can be either direct or indirect loans. A direct loan is negotiated between the ultimate user of funds and the bank. The user must formally make the loan request and support it with personal financial information to borrow from the bank. An indirect loan is funded by a bank through a separate retailer such as an automobile dealer who sells merchandise to the customer. The retailer takes the credit application, negotiates terms with the individual and presents the agreement to the bank. If the bank accepts the proposal it buys the loan from the retailer under prearranged terms.

Consumer Loans

Consumer loans play a key role in the personal financial planning process of an individual or a household. Financial goals are achieved through these loans. The significance of consumer loans lies in successfully managing the credit borrowed, amount of credit to be used and managing the debt-repayment saddle. Consumer loans have become popular in demand because of individuals, household families, etc., who cannot afford to get expensive goods and services from their minimum income. Therefore they depend on loans. A consumer loan may be opted for buying a car or a stove or new clothes or for a vacation. Most of the consumer loans are treated as personal loans and are used for purchasing all major products and necessities except a house. The interest paid on consumer loans is not deducted from the income tax return. While borrowing consumer loans, the approximate monthly budget should be determined. There should be control in the use of debt as it is expensive. If ignored, it may lead to the disturbance of the entire estimated budget that in turn leads to serious problems. Before applying for the

1 Credit card loans and overdrafts are also installment loans, as they require periodic monthly payments. However, they have other different features, so they are discussed separately.

loan, complete credit-counseling needs to done to have proper understanding about consumer loans. These loans must be borrowed from lowest cost source i.e., at a low rate of interest. If all these aspects are not taken into serious consideration it may lead to bankruptcy.

Consumer loans are formal and negotiated contracts which state both, the terms and conditions of borrowing and repayment. They are one-shot transactions given for specified purposes. There is no revolving credit facility once it is borrowed. No checks or any credit cards issued for such loans. Consumer loans have become a part of every household. The consumer should have a proper understanding of what kind of a loan would suit his budget and his own repaying capacity. He should know that greater the maturity of the loan, the greater will be the cost of repayment. Industries, people, companies, etc., lack liquid cash, because of which they prefer loans. These loans have now become a must for meeting day-to-day expenses.

HOME LOANS

One of the most widely preferred and popular loans are the home loans. In India, most people have a dream of having their "own house". To fulfill their dreams they need huge capital that is beyond their monthly income. Therefore, banks and other financial institutions have recognized this need to issue different kinds of loans to their customers. The advantage in obtaining a home loan is that the liquid cash or the savings is not used and the monthly loan installment is minimal and thus affordable. The loan is repaid over a period of time say, 10 years or 15 years etc. The asset is obtained without much expenditure and provides immense satisfaction to the customer. This initiates more and more individuals and households to opt for loans. The risk involved in such loans is minimum. Since the target market is the household and the individuals, the default rate is generally very low. If there is a situation of default then a period of extension is given to the customer. Even then if the customer fails to repay the loan, then the house or the land for the purchase or the construction for which the loan was applied can be seized. To eliminate this situation, the customer should be familiar with the terms and conditions of availing a housing loan.

The appraisal officer states, the entire terms and conditions and also attends to the queries of the prospective borrower. Various details like eligibility criteria, the period of repayment of loan, the interest rates on the loan, the documentation required from the borrower etc., are discussed during this meeting. If the customer is satisfied and proper study is done then the application is filled. The processing fee is paid which is about 1% of the loan amount. This fee is not refundable and is paid only if the chances of getting the loan are really good. The appraisal officer conducts a personal interview with the borrower. He then makes a report and then discusses it with the branch manager. The branch manager substantiates the recommendations of the appraisal officer and then sends it to the competent authority seeking sanction of the loan. The competent authority sanctions the loan and the appraisal officer clears any query for the satisfaction of the authority. If the loan has been approved then the borrower collects the loan offer letter. The property details, form and acceptance note are filled and signed. This implies that the borrower has agreed to the terms and conditions of the loan. The borrower is expected to collect the disbursement within 1 month of the offer letter, if not, commitment charges 1% of the loan generally are levied on the borrower. A 1% fee towards legal and technical fee is also charged. The legal documents are submitted to the legal officer. The loan agreement and other documents are signed. The legal officer prepares a legal report after studying the legal documents in detail. The technical officer visits the property and then makes a technical report. He recommends the amount for disbursement depending upon the stage of completion. The disbursement memo is then signed by the appraisal, technical and legal officer and then sent to the branch manager for his signature. The accounts department prepares the cheques that are to be sent to the borrower with authorized signatories. This disbursement memo is attached with important documents like

the interview sheet, legal report, technical report etc. Interest is charged on the amount disbursed to the borrower and is called EMI. This cheque is collected from the borrower before releasing the disbursement cheque. Consequent to the final disbursement, the borrower starts paying the EMI. This is the interest and the adjusted principal amount for the period allotted. The documents pledged by the borrower are released after the clearing of the loan.

AUTO LOANS

Cars are becoming affordable due to ease and availability of finance and lower interest rates. Considering the economy involved car manufacturers have over a period of time increased the number of manufactured cars. Most people also tend to purchase car regarding it as a status symbol and prestige in the society.

A car loan or auto loan is obtained to purchase a new or a used car. The car is used as a collateral security for availing the loan. The loan period for a new car ranges from 3 to 7 years, while for used car it is shorter in duration. The interest rate for auto loans depends on the period of the car loan, and the credit rating of the buyer. Auto loan accounts constitute 35% of all consumer credit outstanding. Usually 80-90% of the auto loan is financed with credit and the rest is usually the down payment or the initial amount to be paid by the borrower.

There are a number of banks and other financial institutions providing excellent loans suiting the needs of different class of customers. The interest rates on the loans and the period of repayment of the loan are framed such that they are easily affordable by any class of household sector and individuals who satisfy the eligibility. Most of the banks and other financial institutions try their best to grant loans, which fit into the normal budget criteria too. Therefore, they have become more preferable. Two-wheelers are considered more accident prone when compared to four-wheelers. People have become more safety conscious due to fear of accidents. Moreover, a car can accommodate the entire family and since Indians are more family-oriented and move around more in groups, cars are always in demand.

The risk in auto loans is less. If a person is not able to repay then the bank or any other institution from where the loan has been acquired, can seize the vehicle. Therefore, the borrower should calculate his monthly budget carefully and avail a loan. He should also carefully study the terms and conditions of the interest rates, the monthly installments, the tenure of the loan etc. Budgeting is very important as the costs correlated with obtaining the car do not end as soon as the car has been delivered or the loan, paid off. In fact, owning the car is one part of the cost-cycle. Costs constituting repairs, maintenance, taxes, insurance, registration etc., also add to the budget. Therefore, the affordable budget should stretch not only during purchase time but also over the life of the vehicle. The kind of car, the affordable price, the type – petrol or diesel and the expected maintenance costs etc., should be carefully decided by the borrower. He should also decide whether he wants to lease the car or go for hire purchase. In case of lease, the financer or the lessor charges low rate of interest by transferring the depreciation benefits. The borrower gets tax benefits like, lease amount, cost of maintenance and insurance which can be claimed as expenses. In case of hire purchase, the borrower gets the benefit of tax shield on depreciation, as he possesses the car. The amount paid as road tax, interest on loan, insurance, repairs etc., are deductible from the income for income tax calculations. In case the borrower is an individual he is not liable for the tax benefits. After deciding between leasing or hire purchase, the borrower should prefer a loan that suits his repaying capacity and monthly budget. Therefore, he needs to get the rates, terms and conditions of all the companies providing the auto loans. Comparison of the rates, the payment and tenure of the loan, the down payment or the initial payment, the incentives or discounts that the companies offer must be identified. Before signing the agreement for the loan, the borrower should clear all his doubts by asking questions. He should try and get a copy of the agreement. Understanding the important clauses in the agreement or the contract will eliminate troubles in the future.

Most of the finance companies and banks market their loans through dealers or agents. Therefore, authentication of the dealer should be verified. Usually, post-dated cheques should be drawn for the repayment of the loan. Most lenders including foreign banks make the borrowers sign the set of loan documents. Even if one document is missing, the loan will be rejected.

PERSONAL LOANS

This is a type of consumer credit loan. It is an unsecured loan granted for personal use based on the borrower's integrity and ability to pay. Some consumers need additional or extra cash for buying a new computer system or washing machine. According to Jane.C.Yao, Managing Director of American Bankers Association, a banking trade group, personal loans are considered to be a growing market, and banks are finding increasing demand for this product. When the customer is planning to avail a personal loan, he needs to be cautious about few things.

Lower monthly payments are not always good. The customer should never feel keyed up with lower rates. The amount of credit available must be clearly known. The customer should also look into the hidden charges by interacting with the lender frequently. This also helps him to find out if there are any loopholes. Associated fees if any, should be known. Certain information about itemized charges must be known like credit insurance, associated buying clubs and extra cash. The finely printed terms and conditions should be read and complete knowledge about the contract should be gathered. If there is any difference in, what the loan officer has communicated and what is written in the agreement then the customer must outrightly reject the acceptance of the loan and the agreement. The customer should always bear in mind that what is in writing is important and that is what matters when any dispute arises between the customer and the lender. Bigger loans are not always better; sometimes if the loan officer manages to convince a customer for a higher loan then the benefit may be only to the concerned bank in the form of extra commission.

EDUCATIONAL LOANS

Families in India attach lot of importance to providing education to their children. For this reason, though a majority of people struggle to earn their living they still strive to give their children the best education. Since most educational fields have become advanced, many tend to educate their children in these fields. Thus, they naturally require lot of liquidity in the form of cash. To solve this problem, many banks and other financial institutions are now providing a variety of educational loans at reasonable interest rates. So, people have a choice to select the kind of educational loan that suits them the best depending on their repaying capacity. Until a few years back most educational loans were offered to students going abroad to pursue their higher studies. But now, people have the facility to provide quality education in India itself, and save a lot of money. Thus, people are ready to pay for quality education by way of educational loans from banks. These loans are repayable in monthly installments and are affordable.

Interestingly, the idea of selling educational loans was tough in India initially, as people did not generally look for such loans. But now things are changing. As the expenses for education have increased, the youth are not willing to let their parents pay for their education and remain a burden on them. They opt for educational loans and work side by side and the amount thus earned is used for the repayment of the loans. This is advantageous as the youth is learning to struggle and learn to become more independent and responsible. Since educational loans have become part of priority sector lending, formalities involved are reduced and it is easier and cheaper to get them. The lower interest rates are actually the icing on the cake for those availing an educational loan.

LOANS AGAINST SHARES

Sometimes borrowers may pledge their shares and take loan. This provides a collateral security to the lender for the loan availed. If default occurs then the lender has every right to seize the shares and sell them to satisfy the unpaid loan amount. If there is still any deficiency then the borrower may or may not pay.

SINGLE PAYMENT LOANS

This loan is granted to the borrower for a specified period of time, after which he is entitled to repay the entire amount. This amount includes the principal amount plus the interest. The maturity period ranges from 30 days to a year. They sometimes serve as a source of interim finance to pay bills or for purchases when the funds are unavailable but are expected to be forthcoming in future. Sometimes single payment loans are used by those customers who want to avoid the monthly installment payments and choose to make large payments at the end of the loan. Single payment loans are of two types: secured and unsecured, which are availed for any purpose like for going on a vacation or for purchasing a music system or for purchasing a television. Single payment loans help in rebuilding or establishing an individual's credit rating.

BANK CREDIT CARDS

The giant among the open account credit is the bank credit card or 'plastic card'. These cards are issued by the bank or any other financial institution that allows the customer to make purchases at any establishment that accepts it. It is widely used for the purchase of consumer goods and services. The two types of cards that are issued are the Visa and the Master Card. The credit card is now used to pay almost for everything – groceries, cosmetics, assets, doctor bills, hotel charges, college and tuition fee etc. In recent years, big names have emerged in this area like American Express Blue Card, Citibank's Taj Diners Club International, Bank of America's Platinum, Centennial Visa or Master Card etc.

30-DAY CHARGE CARD

They are the regular cards and the customers are expected to pay the monthly bill in full within 10 or 20 days after the billing date. Interest can be avoided if the payment is made within the specified due date. However, interest penalty is charged after the due date. Gas or electric companies or telephone companies etc., offer these kinds of cards. They do not involve the use of charge cards.

DEBIT CARDS

Its appearance is just like a credit card having the logo of Master or Visa. Debit cards enable direct access to a person's checking or savings account. Buying through debit card is similar to buying through credit card. There are no finance charges involved in the debit card. Debit cards have become immensely popular especially among the sector that cannot afford to pay high interest on credit card billing. Debit cards are accessed through ATMs – which offer 24-hour service. Accessibility is easier too for cash advances. The disadvantage with debit card is that it does not provide a line of credit. Some debit issuers charge an annual fee and some merchants charge transaction fee. However, the biggest advantage of debit card is that it does not burden a customer with problems unique to a credit card.

DESIGNING OF BANK MARKETING NEW PRODUCTS AND SERVICES

Competition, securitization, automation and regulation are the major forces that are driving and shaping consumer lending. Net banking, phone banking, mobile banking, ATMs and bill payments are the new facilities that banks are using not only to lure customers but also to help them reduce their total operating costs. In India, commercial banks dominate the market for consumer credit. Even nationalized banks, which control more than two-thirds of the banking business in the country, are tapping retail lending with great vigor. The enormous competition has led to innovative retail banking products that are extremely customer-friendly and plug the loopholes in the existing similar products.

For several years, banks viewed consumer loans with skepticism. Commercial loans dominated the banks' portfolio as they generated high net yields with low credit risk. Consumer loans in contrast involved smaller amounts, large staff to handle accounts and high default rates. The banks considered them substandard. Even the regulators across the globe have not encouraged consumer finance till very recently. However, over the past few years, fierce competition among the banks has lowered the spreads and profitability on commercial loans. With deregulation and increase in consumer loan rates, the risk-adjusted returns in the retail sector have exceeded the returns on commercial loans.

RESPONSE OF BANKS WITH NEWER SERVICES AND DELIVERY MECHANISMS

A few new generation banks have introduced customized banking products like Investment Advisory Services, SGL II Accounts, Photo-credit cards, Cash Management Services, Investment Products and Tax Advisory Services. A few others have also gone into money market mutual fund schemes. Eventually, the banks are planning to market bonds and debentures also. Selling of insurance products by banks, which was considered a distant dream some time back has already become a reality. For example, Aviva Life Insurance has tied up with ABN-Amro Bank to market its insurance products. Banks also offer advisory services termed as 'private banking' to 'high relationship-value' clients.

New distribution channels have transformed the way banking is conducted. More and more banks are outsourcing services like disbursement and servicing of consumer loans, credit card business, etc. Most of the new generation banks have been aggressively selling their products through Direct Selling Agents (DSAs). Home banking, telephone banking and Internet banking have already become common. ICICI bank was the first among the new private banks to launch its net banking service, called Infinity. It allows the user to access account information over a secure line, request cheque books and stop payment, and even transfer funds between ICICI Bank accounts. Citibank has been offering net banking through its Suvidha program to customers. Products like debit cards, credit cards, flexi deposits, ATM cards, personal loans including consumer loans, housing loans and vehicle loans have been introduced by a number of banks.

Corporates are also deriving benefits from the increased variety of products and competition among the banks. Certificates of Deposit, Commercial Papers, Non-Convertible Debentures (NCDs) that can be traded in the secondary market are gaining popularity. Recently, market has also seen major developments in treasury advisory services. With the introduction of Rupee floating rates for deposits as well as advances, products like interest rate swaps and forward rate agreements for foreign exchange, risk management products like forward contract, option contract, and currency swap are offered by almost every bank in the market. The list is growing day by day.

Retail banking includes a comprehensive range of financial products viz. deposit products, residential mortgage loans, credit cards, auto finance, personal loans, consumer durable loans, loans against equity shares, loans for subscribing to Initial Public Offers (IPOs), debit cards, bill payment services, mutual funds, and investment advisory services. These products provide the banks an opportunity to diversify the asset portfolio with high profitability and relatively low NPAs. Today, the most proactive banks have entered the retail banking segment and have identified it as a principal growth driver. They are slowly gaining market share in the retail space.

Table 1: Seven Approaches to Improving Service Productivity

Approach	Philosophy
1.	**Service productivity can be improved if the employees of the organization work more skillfully.** Through better selection and training procedures, the organization can hire and foster more skillful workers.
2.	**The quantity of the service can be increased by surrendering some quality.** For instance, patients admitted for treatment in a healthcare center get due attention from the doctor. However, the same doctor has to handle more patients and give less time to each patient in an Outpatient Department (OPD).
3.	**By adding equipment and standardizing production, the service can be 'industrialized'.** For instance, when it comes to systemized service and low cost, rapid-fire food production, the world's most acclaimed company is McDonald's. Through an assembly-line approach, the company has adopted a 'manufacturing attitude' toward producing services, culminating in the technological burger. The service has been industrialized through a standard kitchen layout. An outlet in Beijing will not take any more or less steps to assemble a burger than the one in Delhi. In addition, a well-planned procurement framework has enabled cost and time efficiency of service.
4.	**Reduce or make obsolete the need for a service by inventing a product solution.** For instance, the emergence of the video cassette recorder (VHS format) in the 1980s affected ticket sales of cinema theaters in India. Later, in the early 1990s satellite and cable television bombarded viewers with 24-hour movie channels. This development reduced the demand for VCRs, and ticket sales of cinema theaters dipped further. With the emergence, today, of high-quality CD-ROMs on PCs, the annihilation of the VCR is practically complete.
5.	**Design a more effective service.** For instance, how-to-quit-smoking clinics may reduce the need for expensive medical services later on.
6.	**Present customers with incentives to substitute their own labor for company labor.** For instance, a restaurant specializing in buffet lunches and dinners is actually replacing employee "serving" labor with customer "self-service" labor.
7.	**Harness the power of technology.** The power of technology not only enables time and cost efficiencies but also makes service providers more productive. For instance, the emergence of mobile phones has dramatically increased the accessibility to the potential client, which, in turn, has improved the productivity of the salesman. Similarly, the accurate and speedy railway computerized reservation system is a far cry from the manual system that it replaced.

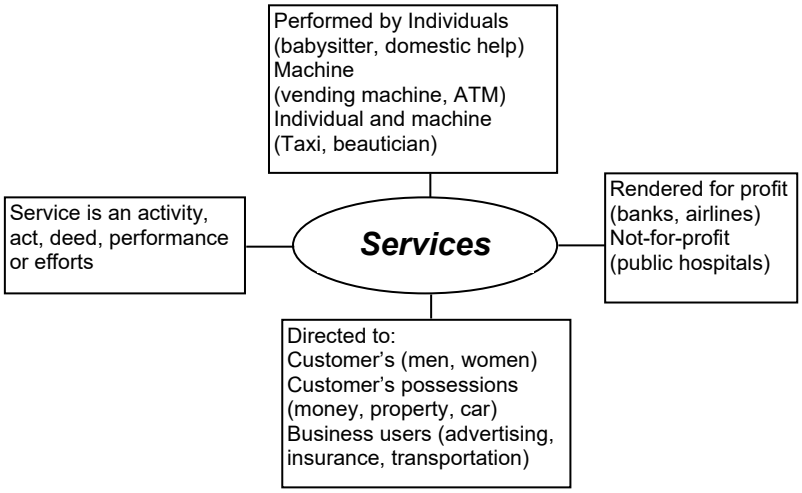
DELIVERY STRATEGIES IN A BANK

The concept of services is complicated, as a service may encompass many features, ranging from a personal service involving a complex relationship to a service more like a commodity with a tangible product, and thus more easily comprehensible. It is in this context that the strategy to deliver a particular service assumes much importance. An example is car rental, where the customer drives the car – a very tangible and comprehensible result of the service offered, whereas in the case of an insurance service, the customer pays for something highly impalpable, namely risk reduction. The insurance company bears the risk, which the customer consumes all the time. Customers, however, do not really comprehend the total context of the service until a loss is experienced. Different

levels of personal interaction are also exemplified in both cases. Car rental is often handled in a "standardized" manner, not necessarily entailing personal contact other than signing a contract and receiving a key, whereas an insurance contract requires a high-level of personal interaction, albeit, at times, telephonically.

The diagram given below, presents a bird's eye-view of the different types of services, how they are performed, the target groups to whom these are directed and the purposes.

Figure 1



The different categories of services:

Process Based

The services can be classified based on the degree of customer involvement.

- **People processing:** The customer has to actively cooperate with the service operation. For instance, healthcare, restaurants, beauty salons, and gymnasiums.
- **Possession processing:** Services offered to physical objects – both live and inanimate – belonging to the customer in order to extend their usefulness. For instance, courier, car repair and maintenance, laundry and dry cleaning, gardening and veterinarian services.
- **Mental stimulus processing:** Services that interact with people's minds to shape attitudes and influence behavior. Due to the customer's dependency there is a potential for manipulation. For instance, psychotherapy, education, professional advice and religious services.
- **Information processing:** Services that are highly dependent on effective collection and processing of information. For instance, financial services, accounting, law, marketing research and medical diagnosis.

Service Tangibility

The degree of tangibility can be used to classify services.

- **Highly tangible:** ATMs, car rental, vending machines, and equipment leasing.
- **Service linked to tangible goods:** Office equipment delivery, installation, maintenance, repair and training.
- **Tangible goods linked to services:** Banks (cheques/DDs), restaurants (food), healthcare (drugs) and management consultancy (final report).
- **Highly tangible:** Psychotherapy, housekeeping, babysitting etc.

Expertise

The expertise and skills of the service provider can be broken down into the following categories:

- **Professional:** Consultancy, medicine, legal, accountancy and teaching.
- **Non professional:** Baby sitting, housekeeping etc.

Profit Orientation

The overall business orientation is a recognized means of classification.

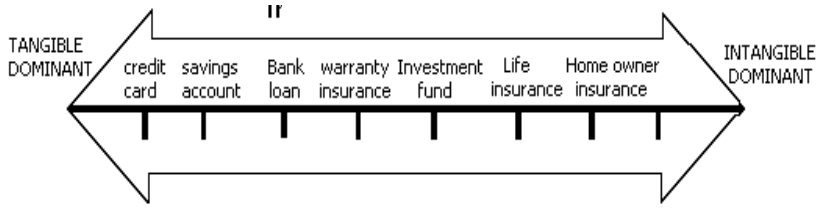
- **Commercial:** Banks, hotels, airlines etc.
- **Not for profit:** Charities, public sector, leisure, facilities etc.

End-user

Based on who consumes the service offered, services can be classified into following categories:

- **Consumer:** Hair dressing, psychotherapy, and medical services.
- **Business to Business:** Advertising agencies, printing, accountancy and consultancy.
- **Industrial:** Plant maintenance and repair, installation and project management.

Figure 2: The Financial Service Continuum



Source: Derived and modified from Cowell, 1984.

The services of a bank are only a part of the service spectrum. However, with the differences between investment bank, commercial bank and insurance firm getting reduced, banks now offer a universe of services. In India, even the NBFCs are offering commercial banking services and commercial banks are offering merchant banking services. For instance, Kotak Mahindra, a NBFC has been permitted by the RBI to offer commercial banking services while HDFC and ICICI offer merchant banking services.

Apart from offering services to retail clients, commercial banks offer services of advisory nature to corporate clients in the form of project financing, venture financing etc. On this front, the services could be classified as fee-based activities and fund-based activities. If a bank provides advisory services regarding underwriting, guarantees, LCs, advisory and consultancy services, Cash Management, investment services, asset management, credit card services, Electronic Bill Presentation and Payment (EBPP) services, mortgage, retail investment, upgraded and expanded Trade payment and letter of credit products and services, it means it is providing fee-based services. On the other hand, if the bank gives loans and accepts deposits, they become fund-based services. Dropping margins of deposits and lending money are making most commercial banks turn towards fee-based services. Income from being marketers of services right from insurance to airline tickets is expected to form a larger proportion of bank's incomes. In developed markets, banks derive as much as 70% of their income from fee-based services. Today a bank also offers asset management products, ranging from mutual funds to venture capital investments.

Another differentiation of services of a bank is that of retail services and corporate services. Retail banks offer services involving the transfer, borrowing and lending of money to private customers and sole traders and partnerships. Commercial banks deal with corporate or commercial customers rather than individuals. Many of the major retail banks have commercial banking arms. Client size can range from small start up companies to major corporations.

Outsourcing Benefits

This is where outsourcing has proved to be an effective solution. Instead of attempting to do it all, banks have been better served by pursuing partnerships and collaborative outsourcing – with this they have a full-service line without the extra expense of investing into related technology or developing a capability in an area that is not core to their historical focus.

A single outsourcing arrangement with a bill management service bureau smoothens the entire process and eliminates the complexity for the bank. A service bureau offers pre-packaged technology and business process management for simple and effective service offerings by banks.

Banks not only gain access to the best-in-class technology and business processes, but also importantly, are able to offer the service to their customers in an accelerated time frame. Outsourced management enables banks to launch their bill payment services, fully operational with the best-in-market capabilities, in weeks rather than months.

Outsourcing the bill payment service management to experienced service bureaus offers banks established alliances, leading edge technology, operational efficiencies, control of processes and assurance of service delivery. Importantly it provides a single, centralized interaction point for the bank and establishes a high degree of standardization for the bank's activities. Banks do not have to worry about developing the business processes, managing day-to-day operations or multiple biller interactions; instead they simply focus on customer management.

A key advantage to banks from outsourcing is the cost-advantage factor. Not only do banks not have to make large technology investments that would otherwise have been required, but they are also able to bring down their fixed costs of operating by leveraging the cost structure of the vendor. The business model and cost structures of service bureau companies are better suited to the realities of the new payments environment than that of the traditional players. Outsourcing helps banks to drive down their costs and match up on competitive ability.

STEPS TO IMPLEMENT DELIVERY STRATEGIES

Service Quality contains two components – Technical quality and Functional quality. While technical quality provides an answer to the question "what", i.e., giving the essence of the service itself, and is objectively measurable, functional quality represents an answer to the question "how." Thus more closely characterizing the manner by which a certain service has been provided and reflects the subjective perception of the consumer. We include into technical quality, such factors as, for example, the depth and width of the product range, know-how, and the possibility to use electronic banking. Therefore for a bank, technical quality refers to 'what' the bank gives the customer while functional quality refers to 'how' the bank's services are provided to the customer. Typical factors, which influence functional quality are: speed, courtesy, and in the case of electronic banking services, in particular, simple access and transparency. Both qualities are linked and together with the image of the given financial services provider, which represents a certain relationship to the past, these create the final service quality.

The 4 steps approach, which is given below, can go a long way in helping a bank achieve its quality goals. These steps are also discussed in greater detail.

Determining What Satisfies the Customer

This is the most crucial and perhaps, the most difficult part of the exercise. The best way to determine what satisfies the customer is to ask the customer. Several organizations regularly send out questionnaires and direct mailers to their customers (both internal and external), analyze the feedback received and initiate appropriate action.

Varying Customer Perceptions of Banking Service Quality

'Customers', who are central to the banking service, are not a homogeneous class. They come from varying socio-economic and cultural backgrounds. The perception of the quality of banking services provided will differ from customer to customer and even for the same customer at different points of time, depending on the mood and mindset of the same user at a particular point of time. A customer who needs money and comes to an ATM on a Sunday to find that it is not working is likely to be much more dissatisfied than if she/he were to find the same ATM temporarily out of order on a working day. Some other factors that may influence perceptions of banking service quality are:

- Overall ambience at the bank.
- Past experiences with the bank.
- Familiarity with the services offered by the bank, the procedures followed etc.
- Knowledge of or experience with competitors' products and services.
- Banking with a particular bank may be regarded as a status symbol.
- Interaction with and/or opinions of other customers' rights etc.

These factors make the measurement of banking service quality difficult and subjective.

Devising Quantitative Determinants

Based on various feedback results and on the bank's internal research, a bank may devise suitable quantitative measures that can be tracked regularly. After the system of tracking has stabilized, suitable standards can be set. Interface with customers results in several "perceptions" that must be handled every day. A bank must ensure that these result in total customer satisfaction. For example, a bank's Customer Service Standards may stipulate that all incoming phone calls be answered within three rings, all queries be attended to within five minutes, no call be transferred more than twice, all messages be recorded and communicated to the concerned person/department within thirty minutes, etc.

Today, it is estimated that there are over 1500 banking websites, with the growing importance of the Internet; banks will have to formulate standards for Internet interface also. These could be, for example: all queries to be answered on e-mail within 12 hours and to be followed up with written communication within 24 hours, etc. Where there is direct interface with the bank's employees, it must be ensured that all customers get a maximum sense of satisfaction. Many banks have set standards, for example: not more than three people should be waiting in a queue at any counter, all those in the queue should be attended in 3 minutes, all deposits should be accepted and receipt issued in 10 minutes, etc. A bank should attempt to formulate Quantitative Determinants to enable objective measurement of various parameters. A few quantitative determinants that could be used by a bank included in its retail banking, corporate segments are:

RETAIL BANKING

Quantitative determinates could be, for example, time taken to

- Accept a cash deposit
- Accept a cheque deposit
- Complete a cash withdrawal
- Complete a cheque withdrawal
- Act on an account-opening request

- Open an account (provided everything is in order)
- Issue a draft
- Issue a cheque book
- Issue an ATM card
- Issue an account statement
- Give a locker
- Update a passbook
- Clear an outstation cheque
- Answer routine customer queries on account balance, cheque clearing status interest rates etc.
- Answer other customer queries on forex rates, etc., which may require information from other departments.

The following would also give the bank a fair assessment of the internal customer service standards prevailing at its branches:

- Complete voucher checking and posting
- Sanction overdrafts
- Processing of consumer loans etc.

These are all time-based determinants; it may also be possible for a bank to devise cost-based determinants in some of the above cases. However, a cost based determinant is often highly dependent on other factors like the position of the bank. Additionally, it may inadvertently shift focus of the exercise.

CORPORATE BANKING

Quantitative determinates could be, for example:

- Total time taken to process a loan application.
- Time required for disbursing a sanctioned facility.
- Time between the taking of the decision and it being conveyed to the concerned party.
- Number of questions/documents to be provided for a loan request to be processed.
- Time taken by the customer to access the correct person in the branch.
- Number of reference made by the corporate office to the branch before an application can be processed.
- Number of days taken at the corporate office to process a proposal.
- Number of follow-up efforts made to recover loans from defaulters.

These could be compared and benchmarked against similar figures for competitors.

OTHER DETERMINANTS

Quantitative determinants in other crucial areas could include:

i. Number of complaints received per period month, quarter, etc.
ii. Percentage of repeat complaints or complaints inadequately handled.
iii. Percentage of complaints pertaining to attitude of employees, transaction processing time, excessive charges, wrong debit entries etc.
iv. Percentage of ATM down time.
v. Percentage of system down time, maintenance time, etc.
vi. Percentage of customer space to total space at the branches of the bank.
vii. Ratio of employee turnover at the bank to the industry average.
viii. Average number of training hours provided by the bank.
ix. Average number and volume of exceptions reported per period.

CUSTOMER COMPLAINTS

Generally, it is found that customer complaints relate to one of the following areas:

i. Deposit accounts, non-payment of interest, fraudulent withdrawal, transfer of funds, wrong debits, etc.

ii. Delay in collection of cheques, drafts, etc.

iii. Non-issuance of duplicate drafts, etc.

iv. Grievance relating to remittances.

v. Failure to honor or delay honoring invoked LCs guarantees etc.

vi. Delay in the sanctioning of loans and advances, charging of higher interest rates, etc.

vii. Miscellaneous complaints.

As can be seen, most of the complaints relate to retail banking transactions. A bank could find it advantageous to focus more attention on introducing quantitative determinants for retail banking areas.

Box 1: Quality-not Quantity-of Management

Today's pacesetter companies do not view their strength in enabling growth in terms of the quantity of management of the hierarchical leadership of an earlier day, instead, they emphasize the quality of management, which recognizes and is measured in terms of leadership and networking capability for focusing a company's total resources on sustaining business growth.

They implement these results through effectiveness in developing and deploying management capital's intellectual, technical, human information, and other resources in integrating the company's "hard" and "soft" assets. This takes place through the processes, tools, and strategies that help each man person in the company think, learn, act, and make decisions about how he or she both or individually and as part of a team can help provide the superior value for customers and, consequently, for investors that meets today's accelerating business demands.

The objective is not to increase the emphasis on additional managerial techniques nor to establish a few more high-level management departments on the company's organization chart nor to create a new systems bureaucracy. Instead, the objective is to create constant momentum for establishing and maintaining competitive leadership in all – not just some, as in traditional old-economy companies – the principal management channels across the company's business wine chain.

These channels include product development, supply management, operations effectiveness, and quality, as well as others. These principal management channels facilitate a company's leadership effectiveness so that the company can better use not only its financial and physical assets but particularly its human, technical, intellectual and informational resources for better planning; better care of the company's customers; and better creating, selling, and delivering of the products and services for those customers.

Essentially, this quality management leadership emphasis develops, implements, and maintains systematic capabilities that establish, align, and integrate a company's strategy, objectives, goals, and measurements with its work, teamwork processes, and execution tools. It does this in all the company's key business areas. It is the foundation of an organization's balanced – not piecemeal – approach to leadership, and it prioritizes a company's actions throughout the full scope of its improvement opportunities and requirements. It is fully integrated with the company's drivers of sales-revenue.

The key point is this: It is the attitude, process, and management capital disciplines that create the structure and organization for this quality of management emphasis – not vice versa. Furthermore, the management capital structure may vary among companies because it is determined by each company's history, markets, personality, and requirements.

Source: http://www.expressitpeople.com/20040809/management2.shtml

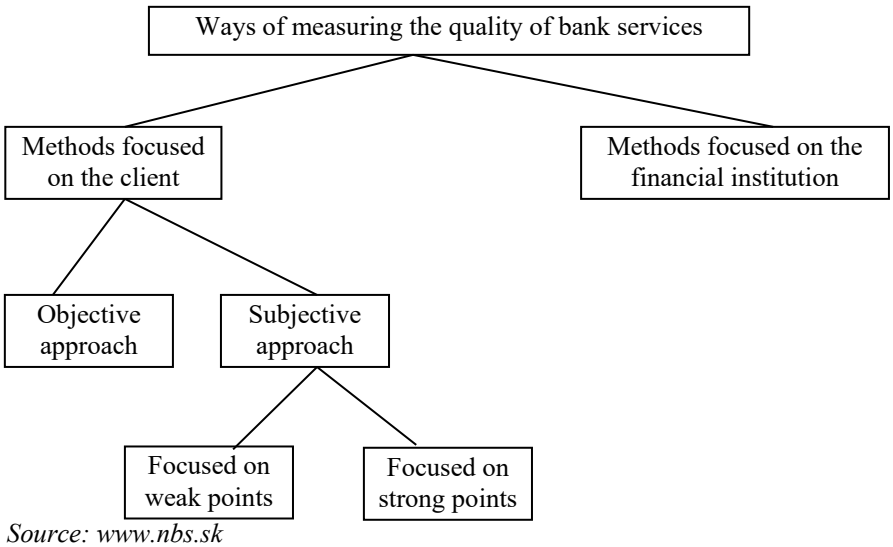
Non-Quantitative Determinants

A bank can also devise various non-quantitative determinants to help it improve its service quality. This is necessitated because the objective and scientific measurement may not always be feasible or practicable. Non-quantitative determinants can also throw additional light on various facets of the bank's service quality: some of the areas a bank can focus on include branch premises and customer lounges, ATMs, technology, publicity, and bank's staff members.

Non-quantitative determinants are often difficult to standardize or benchmark. In some cases, however, internal guidelines standardize ATM premises, branch premises, handling of customer complaints, questionnaires used to obtain feedback, etc. Many factors, like the customer services, orientation of staff members may be difficult to evaluate and in case of staff there is need to standardize recruiting policies and procedures to ensure that the right kind of people are selected. The bank could also experiment with various tests – psychological tests, studying behavior in relation to group, etc., to select the right person. As the validity and efficiency of these tests are often hotly debated, the bank must use them with caution and after careful analysis. The bank should then evolve suitable training programs to ensure that there is no effort lacking on the bank's part in equipping the selected candidates to perform their duties satisfactorily.

Non-quantitative determinants are very important because there is no mechanism to gauge where the bank went wrong. There will normally be no complaints relating to these factors, except if the staff has been extremely callous or rude. The effect of these factors on the customers' perception of quality is also difficult to ascertain. Further, the divergence in customer perception is more pronounced for these non-quantitative determinants compared to the quantitative determinants. It is therefore important for a bank to pay adequate attention and attempt to reasonably standardize these factors with the focus being on providing timely and cost-effective quality services.

Figure 3



Source: www.nbs.sk

As competition increases, quality will become the only true differentiator in services. Successful banks will be those that compete on quality. Banks must realize that competing on price means that they are dependent on what the

competition is doing, for their success. Competing on quality means staying ahead of the competition. Banks that wish to surge ahead successfully into the new millennium would need to ingrain a Quality Culture. Every aspect of the bank's functioning would have to be governed by the quality principles.

DESIGNING OF SERVICE QUALITY

Services have a number of distinctive characteristics, which differentiate them from goods and have implications on the manner in which they are marketed. These characteristics are often described as intangibility, inseparability, variability, perishability and the inability to own a service. The following are the four most commonly attributed characteristics of services:

INTANGIBILITY

A pure service cannot be assessed using any of the physical senses – it is an abstraction, which cannot be directly examined before it is purchased. A prospective purchaser of most goods is able to examine the goods for physical integrity, aesthetic appearance, taste, smell, etc. Many advertising claims relating to these tangible properties can be verified by inspection prior to purchase. Services in turn are said to be intangible – they cannot be seen, tasted, smelt or touched, but can only be experienced by customers. A service offering comprises deeds, performances and efforts and therefore is consumed and not possessed. For instance, a management consultant does not dole out anything tangible. The consumer merely consumes the advice given to him. The level of tangibility present in the service offer is derived from three principal sources:

i. Tangible goods, which are included in the service, offer and consumed by the user.

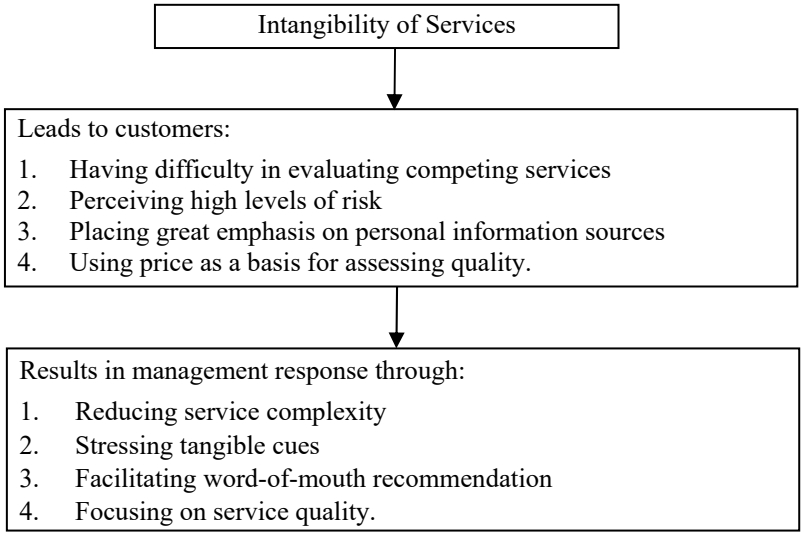
ii. The physical environment in which the service production/consumption process takes place.

iii. Tangible evidence of service performance.

This is true of banking services and most other financial services where the service offered is only what the customer experiences fleetingly. Where goods form an important component of a service offer, many of the practices associated with conventional goods marketing can be applied to this part of the service offer. Restaurants represent a mix of tangibles and intangibles and in respect of the food element, few of the particular characteristics of services marketing are encountered. Therefore, production of the food can be separated from its consumption and the perishability of food is less significant than the perishability of an empty table. Furthermore, the presence of a tangible component gives customers a visible basis on which to judge quality. According to Saner, Olsen and Wyckoff, "Design of the service package and control of design require a greater understanding of consumer psychology than for manufactured goods because of the intangible and often non-explicit nature of the product. The intangibility factor makes it difficult for consumers to measure service value and quality".

IMPLICATIONS OF SERVICE INTANGIBILITY

Figure 4



Source: Principles of Services Marketing; Palmer and Adrian.

The tangible elements of the service often comprise not just those goods, which are exchanged but also the physical environment in which a service encounter takes place. Within this environment, the design of buildings, their cleanliness and the appearance of staff present important tangible evidence which may be the only basis on which a buyer is able to differentiate one service provider from another. For instance, the décor of a bank, the ambience of a restaurant, the infrastructure in a college or the qualifications and eminence of a management consultant are ways to measure the quality of the service. Service providers try to make service offerings tangible by qualifying them with evidential terms called "service marks."

Inseparability

The production and consumption of a tangible good are two discrete activities. Inseparability occurs whether the producer is human – as in the case of health-care services – or a machine (e.g., a bank's ATM machine). The service of the ATM machine can only be realized if the producer and consumer interact. In some cases, it has been possible to separate service production and consumption, especially where there is a low-level of personal contact. Inseparability has a number of important marketing implications for services. Firstly, where goods are generally first produced and then offered for sale and consumed, inseparability causes this process to be modified for services. They are generally sold first, then produced and consumed simultaneously. Secondly, while the method of goods production is to a large extent (though by no means always) of little importance to the consumer, production processes are critical to the enjoyment of services.

Another aspect of the inseparability factor is the high degree of interaction between the provider and the consumer. The consumer always measures the quality of service by analyzing the technical competency of the service provider. In addition, an important component of good service quality is the marketing and interpersonal skills and the service provider. For instance, though a teacher may have sound knowledge in his subject, lack of proper communication skills might leave the students confused. Similarly, slight misbehavior by a receptionist at a hotel may turn-off the customer forever. This is however not evident in purchases of goods as customer satisfaction depends mostly on the functional aspects of the product.

Banks underwent a major transformation in the 1990s. Customer service programs were sharply scrutinized and reviewed. Service quality issues and service quality gaps were identified with increased emphasis on the management of service quality. This has been accompanied by a more disciplined approach to customer and market research.

In the last few years, due to the rapid growth in telecommunications, we have seen the world shrink before us. To counter this revolution, banks will have to re-engineer and redefine themselves. One strategy would be to integrate past efforts within a relationship-marketing context. Relationship marketing is about building and maintaining relationships with all the organization's external interfaces. Customer relationships should be maintained even after the service delivery is completed, and the focus should be on retaining customers, rather than simply trying to attract new ones. Accordingly, Adrian Payne has enumerated the following evolutionary challenges awaiting both bankers and other service marketers:

- Shift emphasis towards a marketing-oriented culture.
- Carry-out market planning in a more disciplined, realistic, and focused manner.
- Integrate various marketing initiatives.
- Emphasize the use of database marketing techniques.
- Increase profitability through improved customer retention.
- Recognize the potential of external marketing, internal marketing, and relationship marketing in a service encounter.

Box 2: Changing Face of Services Marketing

In a world full of uncertainties and upheavals, the realization is fast gaining ground that if you continue to do business today with the methods of yesterday, you are bound to go out of business tomorrow. The decades of the 1980s and '90s have witnessed a paradigm shift in business. In order to remain competitive, companies have attempted to re-engineer their key business functions like production, distribution, after sales service, and so on.

But one core business, which has not moved with the pace of change, is marketing. The limitation is more pronounced in the area of services marketing than in any other sphere.

The services marketing arena today is marked by the emergence of the new generation customer – a global citizen who is more exacting and individualistic, change seeking and value conscious. His purchase preferences transcend national and cultural barriers. He shares a consistent set of tastes and preferences, and the growing commonality of his tastes across the globe qualifies him as a member of a genuinely cross-triad, upper bracket global market segment. Marketing professionals need to develop a keen insight into this global citizen's purchase preferences, attitudes and value expectations, and reorient strategies accordingly.

The value seeking customer today is conscious of and responds to the broader issues like environmental protection, human values and so on. In such a situation, the customer is more inclined to buy cars, which conform to Euro-V emission standards or buy a cola that comes packed in a biodegradable bottle. The same strain runs through the services industry also.

If a credit card company is seen contributing part of its earnings to social causes like blind relief, literacy development, etc., the customer is decidedly going to declare his preference for the same. Similarly, the value conscious customer is certainly going to express his preference for an insurance company seen to be promoting health awareness and research, or is perceived to be contributing its funds for nation building. Here, there is a lesson to learn for the marketing organizations.

Unlike the unique sales proposition of yesteryears, marketing today embraces an integrated value proposition. In the service industry particularly, where often the customer has a long-lasting brand relationship, managing the customers' experience processes is as important as the product being sold and the values attached to it. Today's brand strategies have to focus on providing the best brand experience at the lowest possible cost. The concept of brand experience permeates every product and service. Increasingly, in the brand conscious market, brand differentiation is being determined by the intangibles embedded in the brand offering. To illustrate the point from the hospitality industry, while the basic infrastructure remains the same in different hotels, it is the experience chain undergone by the customer, which brings a touch of life to the brand. Ultimately, it is this experience process that determines whether the customer would maintain the brand relationship or not.

Increasingly, in the service industry, the realization is gaining ground that more than the capital or the infrastructure, it is the people who are its greatest assets. As Herbert Greenberg, founder and CEO of Caliper Inc., would put it, "Global competitiveness is so intense today, and there is so much sameness in products, that you will succeed or fail 98 percent of the time because of your people." In order to maintain their brand competitiveness, service organizations have to necessarily invest in development and empowerment of their own people.

Source: The Economic Times.

SUMMARY

- The marketing of banking and insurance services in India has still a long way to go especially since there is a huge untapped market.
- Due to the competition introduced by the liberalization process, the existing and the new entrants will have to be conscious of the changing market requirements.
- The recent years have seen a drastic change in the banking services as banks are now becoming more customer friendly.
- Technology has introduced revolutionary products like Home banking, Internet banking.
- Most of the banks are now becoming one-stop shop for the various financial services. Further, the quality of service has also risen sharply even in the public sector banks due to the competitive forces.

Chapter III

Introduction to Electronic Banking

After reading this chapter, you will be conversant with:

- Electronic Banking
- Electronic Banking: Market Assessment
- E-Banking: An Introduction
- Internet: E-Commerce, E-Banking
- E-Banking in India
- Internet Banking Strategy
- Risks in E-Banking

Introduction

The world is changing the way it works. The process of globalization has taken everything in its hold. Existing ideas are fast becoming obsolete. New ideas and new economic thinking are taking over the world. Technology is considered to be the prime factor in leading the change. Its impact has influenced and is pervasive of all sectors of the economy. The millennium has started with new challenges and opportunities hidden in the unknown treasure of time.

Technology is a very dynamic force. It is changing the competitive landscape of the financial services and banking industry and is influencing the way their products and services are sold and delivered. The first technological revolution transformed the manufacturing and agricultural sectors. This sustained technological evolution has led to the information revolution. Today, we are in an information era. And information of all kinds is transmitted easily, inexpensively and instantaneously around the world, providing faster access to anyone with a laptop computer, cellular phone or Palm Pilot.

The banking infrastructure experienced changes at many levels and paved a way for the development in information technology. Technology has moved from being a mere tool of automation for existing functions to being a key factor in organization of institutions, an important tool in decision-making process and a major element in delivering services to customers.

The impact of this change is as fundamental to banking and financial services sector as the first technological revolution was to the manufacturing sector. Technology firms have understood the technological needs of the banking industry, and bankers also have recognized the role of technology in the development of banking industry. Today, banking and financial services sector have emerged as one of the driving forces behind the development of information-based technologies.

In India, banks and other financial institutions are enjoying unprecedented opportunities as a result of economic expansion. As economic reforms have set the focus on value to the investors, the banking industry, along with other sectors, is emerging more efficient and competitive. Banking industry has made significant progress in recapitalizing banking systems, in eliminating problem assets from the balance sheets, and in improving supervisory and regulatory frameworks. As a result, the economy is growing, equity markets are rebounding, and foreign capital has started flowing back to India.

Impact of Information Technology

The digitalization of information has facilitated the convergence of once-separated industries into a new amalgam of production, distribution and consumption activities. Computers, telecommunications, television and the Internet are coming together into a single environment using IT. The steady introduction of computer technology in every sector and field ranging from health to business to education is bringing revolutionary changes in these sectors.

INDUSTRY

Information technology can be used, by an organization, to develop products, services and other capabilities that will enable a firm to pull off strategic advantages. The operational and managerial processes can be streamlined with the help of IT; by improving business processes, the organization can cut costs, improve quality and customer service and develop innovative products. The process of manufacturing can be automated and improvements can be made using computer-aided design, engineering production, and manufacturing resource management technologies. IT is able to connect manufacturers with dealers and suppliers in the automobile sector. The organizations are able to use Internet, Extranet and other networks to interact with intra and inter organizational units. Improving business processes will enable manufacturers to enhance their efficiency in production, distribution and sales.

Manufacturing Information Systems help companies simplify, automate and integrate several production activities. For example, Computer Aided Engineering and Computer Aided Design (CAD) help engineers design better products. Materials requirement planning system helps in planning the material required for production process. This is integrated with production scheduling and shop floor operations. This is popularly known as Manufacturing Resource Planning (MRP).

Computer Aided Manufacturing (CAM): These systems automate the production processes. Monitoring and controlling the production processes through Manufacturing Execution Systems can accomplish the automation of the production process. This can also be done by directly controlling a physical process (Process Control), or a machine tool (Machine Control), or machines with some human-like work capabilities (robots).

Business

The objective of using information technology in business is to improve business performance. This may involve improvements in the efficiency of operations, in the quality of the management processes and even in the way the business is conducted or organized. Businesses are benefited in many ways by the use of information technology. Performing various functions, solving business problems and pursuing business opportunities are some of the many benefits. Since organizations are goal-oriented, there should be a clear understanding of the type of information to be collected, stored and analyzed. Management of these organizations can be categorized into top, middle and lower levels. Due to the difference in the nature of decisions taken at different levels of management, their information needs also vary. This information should also be consistent with the requirement of the organizational level at which it is targeted. Tracking the operations involves searching the massive amounts of data in their computer; which is facilitated be the business intelligence software. Following are some of the major applications of the software:

- Data analysis
- Reporting
- Data warehousing.

Information systems in many large organizations are combinations of various functional information systems. Product development, production, distribution, order management, etc are some business processes supported by them. Strategically sharing informational resources to achieve efficiency and effectiveness in business processes can be done by the use of Information technology. Concepts like Enterprise Resource Planning (ERP) and Supply Chain Management (SCM) have evolved out of such needs.

Education

The impact of IT revolution is felt most strongly and immediately in the fields of education, training and research. With the help of communication networks, it is possible to transmit different types of service to diverse audience via a single channel. Thus, improved version of education and other services reach the target groups and special audience. Know-how, ingenuity and innovation based on high-quality education, training and research are key criteria to the success in international competition. Such knowledge and adequate know-how lead to increased economic activity and more jobs.

In this technology driven world, education and training throughout, working life becomes increasingly necessary. There is a need for universal working and problem-solving. The change from one-for-all education to life long learning can be supported by Internet and World Wide Web technologies. Teaching has become more learners oriented. In online learning mode, communication between the trainer, learner and the peers is accomplished through the use of e-mail, online discussion groups, video conferencing, etc.

Scientific and technological research projects, which involve complex mathematical and statistical calculations, make use of IT.

Any course of instruction can be delivered using computer as a primary source. A Computer Based Training (CBT) course may be delivered via a software product installed on a single computer or through corporate or educational intranet or over the Internet. CBT can be used to teach almost any conceivable subject.

Medicine and Healthcare

IT has enabled creation of state of the art diagnostic technology. Ambulatory monitoring, SPECT imaging, Rotablator are various tools used to keep a watch on the heart of a patient. Other diagnostic tools such as Magnetic Resonance, Computer Scanners, and ultrasonic scanners are also used for monitoring patient's health.

The tight coupling of surgical and imaging quality help doctors work more accurately in the operating room. In drug development, cheaper computing power is giving scientists an affordable and powerful tool to understand precisely how a disease starts, and evolves, since they can now test endless biochemical permutations for toxicity and efficacy.

Pacemaker is one of the implanted medical devices with sensors that detect when a patient is exercising and adjust heart rhythm accordingly. Microprocessor controlled devices with embedded technology are used in artificial limbs to sense movements and control the movements of these limbs.

Maintenance of a patient's health record is made easy. A database of diseases, their symptoms along with remedial measures will be of great use to doctors to identify the possible cause and suggest the correct treatment.

In the new world of high-tech medicine, doctor's mind melds with machines, drugs are targeted at tumors and surgeons rarely use their own hands to make a cut. Improvements in medical imaging make the body's inner workings transparent to a degree unimaginable even a decade ago.

Government

Various government and public services are automated to enhance customer satisfaction. Using satellite imaging and mapping identification of natural resources, flood affected areas and the intensity of the effect of natural calamities is almost done instantaneously and accurately. From the census data, identification of beneficiaries of welfare schemes can be easily done using IT tools.

Processing and transmission of data is done efficiently with the help of IT. Various data related tasks are automated to improve productivity of the physical processes. By automating the government services like railway reservation system, land registration system, etc the life of common man has been made easy and smooth.

Defense Services

Information Technology plays a vital role in the Defense Sector. Defense R&D exists to support the armed forces. Their mission includes gathering geographical information, providing expert knowledge and advice to decision-makers in the defense department to enhance their ability to make informed decisions, pursue research and development and contribute to the success of military operations. A few notable applications in the Defense Sector are:

i. An improved view of the underwater tactical picture is produced from the information from a variety of sensors, and platforms.

ii. Surveillance satellite systems provide multi-spectral remote sensing from space for earth resource management activities and intelligence collection purposes.

iii. Improved Landmine Detection systems are being developed using IT and also to neutralize landmines using high-powered microwaves.

iv. Trajectory models and simulations are designed for the efficient working of guided and unguided weapons.

v. Simulators like SAPHIRE, provide a state-of-the-art synthetic environment for air-to-air combat.

vi. Computer based systems are used to detect and characterize threatening biological clouds from a safe distance.

vii. Soldiers equipped with latest hi-tech weapons from rocket launchers to semi automatic rifles to night vision glasses have an edge over their enemies.

Security

Security is a broader issue requiring integration with a variety of support services. IT is widely used in surveillance, security and monitoring which form a spectrum of services. Automated production lines, live stock movement, water supply, weather pattern and work place safety benefit from remote video surveillance.

From weapon analysis to handwriting samples to shoe and tire impressions, IT plays a major role. The high processing capabilities are used in fingerprinting, DNA profiling and toxicological analysis. The plethora of the surveillance and detection systems is mind-boggling. To detect intruders and to put a check on illegal operations - cameras, metal detectors and image scanners are used in many organizations.

Management of Organizations

Information is a vital resource for an organization and needs to be managed carefully. The effective use of information and its impact can be seen in all spheres of life.

With growing awareness about scientific principles of management, impact of globalization and increasing competition, business organizations and their information needs have undergone a great deal of transformation. A management support system that facilitates day-to-day operations in an organization is called as Management Information System (MIS). MIS makes use of computer-based systems for converting data into information. They can be classified into strategic, tactical and operational information systems based on the nature of information and decision structure. Online analytical processing popularly known as OLAP is used for analyzing data stored in the database. Decision Support Systems (DSS) help the managers in decision-making, which are developed using analytical models, specialized databases, and the knowledge and experience of decision-makers. Executive Information Systems (EIS) enable online access to relevant information in a comprehensible format. These systems provide timely, accurate and relevant information to the management. Information systems for strategic advantage are used to gain competitive advantage with the help of information technology. Improving business processes, Business Process Reengineering (BPR), virtual organizations, knowledge management and use of Internet technologies are some of the competitive advantages that companies can achieve.

Economy and Individuals

Developments in IT enable the country to be a part of knowledge-based networked world. It boosts the economic growth of the country, which in turn relates to individual development. The use of IT has resulted in improved production and management process as a result of which the individuals in the society are able to receive higher quality of goods and services.

IT-enabled services provide better quality and timely service to the needy in the society. Using IT, better health services can be provided, which improves the quality of the life of individuals. The Entertainment industry now provides high quality recreational facilities like video games, animations, and computer graphics which enable the common man experience the world of virtual reality.

The use of information by unscrupulous individuals, hacking, virus attacks and computer related frauds depict the darker side of the improvements in IT. Hence, the Indian government has addressed the concerns regarding online transactions and computer related crimes by passing the IT Act, 2000.

Technology has provided individuals access to remote information and interactive electronic communication. For example, many people pay their bills, manage their bank accounts, and handle their investments electronically. They also allow people to inspect online catalogs of various companies, thus increasing the popularity of home shopping.

IT has enabled the cheapest and fastest way of synchronous as well as asynchronous communications, such as e-mail and chat. Video conferencing makes it possible for people located in different countries to have virtual meetings.

Financial Services

The service sectors such as Banking, Insurance, Leasing companies, Investment consultancy, Stock exchanges, Share registry and Custodial services offer financial services to the customer. Most of these services require storage and processing of huge volumes of data. The vast processing capacity of computers along with the latest communication technology enables these companies to operate efficiently.

i. The day-to-day transactions in banks and insurance companies are automated which provide better service in processing transactions.

ii. Better customer service is provided using various IT aided developments such as introduction of ATMs, Magnetic Ink Character Recognition (MICR) cheques, credit cards, debit cards, smart cards, digital e-cash and electronic funds transfer. These developments have helped reduce the transaction processing time and also have made available the services to the customer at a convenient place.

iii. The advent of online transactions, speedy and secure payments settlement have lead to the globalization of financial services.

iv. With the help of satellite communication and software tools organizations like Reuters, Bloomberg and Telerate provide online data related to current developments in financial services.

The performance of organizations has improved with the use of IT. They are able to make better controlled and coordinated decisions. Better information about customer enables organizations to provide Value Added Services. Banks can provide assistance to companies in investments by collecting and organizing data relating to present and future financial position of the company. Use of ATMs, Credit Cards and other advanced tools made the process of withdrawals and payments easy.

Emerging Trends

Shifting customer demographics and developments in new technology are bringing major changes in retail banking. Traditional branch banks are facing a surge of competition from other financial services providers wishing to expand into banking, as also from new entrants into the financial sector.

As technology makes the dissemination of information easier, an increasing variety of distribution channels are emerging. Throughout the world, financial service providers are looking towards a new concept of ‘anytime, anywhere, anyhow’ banking, which demands that retail banks of the future find better ways of delivering a complete set of lifestyle-based financial services which simplify their customers’ lives and allow them have more personal time.

The market for retail banking products and services is very large. The provision of such services is not limited to retail banks alone. Insurance and loan companies are also part of this market. Traditionally, much of the business has been conducted within separate, specialized financial services sectors; as retail banking expands to provide a wider and complete range of financial services to the customer, many of these separate businesses are converging.

During the period of market transition, traditional retail branch banks must finance the costs of change, ward off increasingly serious competition and continue to earn profits if they are to survive. Their ability to successfully manage their businesses through such a difficult period is likely to prove a significant challenge.

Box 1: Electronic Banking Market Assessment

Electronic banking is not a tidy product or service which can be described and confined easily. In some way the electronic banking has been with us ever since the first computer was installed in a bank. The development of electronic clearing of payments through BACS and CHAPS in the 1960s was the first step in the development of the electronic bank. But, was entirely invisible to the customer and to most of the staff.

The payment clearing system has evolved very fast since the deregulation of cross-border flows of funds, the development of capital adequacy ratios, and the imminence of the Euro. The Bank of England was heavily involved in developing a system for real time gross settlement, which would achieve the instantaneous transfer of money.

The cost of handling cash and cheques provided the stimulus for electronic banking and created the hope for dematerialization of money. Shrinking of margins and the new competition between financial services have also paved the way for electronic banking.

Business organizations are conservative in their habits, and will give up cash and cheques only when banks offer them something better. Some bank may decide to make things easy for its customers by offering them a personalized service or a software provider can also deliver a personal banking package like Quicken or Microsoft Money and pose competition to the traditional commercial banks.

Telephone banking is very common now, though the level of service being offered is variable. A major bank may have created a central call centre for personal customers to enquire about their accounts, because the records have been centralized and the staff has been rationalized so as to reduce branch staff. A few banks are already offering a full telephone banking service rather than a promise to look into problems the next working day.

Around the world, Internet or online banking has been available for the last 15 years, and the proprietary systems are good in their way. But their customers are locked in. Of the open Internet-based financial services currently available, majority are simple sets of web pages providing customer information along with account checking facilities. Full Internet banks or self-help financial software packages like Quicken can develop and survive.

The Internet banking will be a part of a range of services offered by banks to their customers, who will have different financial needs at different stages in their careers, or according to their lifestyle. The coming years are likely to see most banks introducing Internet services, introduce digital TV or mobile telephony banking, complementary to their other channels.

The evolution of plastic and chip cards proved advantageous to the banks in that the number of small payments being made is cut, thus lowering transaction costs. The card can be used as a branding or marketing opportunity.

However, the imposition of charges, by some banks, on people using the new media is hampering the technological change in banking sector. Some banks impose a charge, even if they want to encourage use, and in the case of credit cards they charge an extortionate rate of interest. Charges for Automated Teller Machine (ATM) use are a growing practice by some banks that object to the 'free rider' habits of fledgling services, as they rely on the expensive ATM network to provide such services. Another brake on development is that the senior management of the major banks is itself over the 45-year old, cut-off age for acceptance of the new technology. At this age they probably do not understand what the technology can do, how quickly it can do it, and the implications of doing it. Bankers who do not understand how their business is run are likely to experience trouble in future.

Source: ICFAI Research Center.

Box 2: Lifestage Marketing in Financial Services

At a time when competition is intensifying across the financial services industry increased pressure is put on margins and profitability. By understanding the customers' needs, they can be targeted more effectively and as a result product take-up and profitability can increase.

Lifestage marketing is about marketing specific products to customers in a way that is related to the stage of their life they are in. This is based on the assumption that certain events or moments in people's lives trigger particular needs or desires. The success lies in recognizing these changing priorities as quickly as possible and targeting the customers, whether existing or potential, with the relevant products. With the help of information that financial services companies already have, from existing customers, it is easier to find out what to target, to whom and when. In this way, customer take-up should increase, as customers are only marketed products that they need when they need them and are thus more likely to pay attention to anything that is presented to them. Lifestage marketing is a good way to attract attention to the product, as it relates specifically to what is happening in the customer's life. When done correctly and used in a way that is consistent with the company's brand, lifestyle marketing should form a highly successful acquisition and retention tool.

The concept of lifestage marketing will be of interest to anyone involved in the retail financial services industry. Issues and future trends in this area should be of interest to those planning their strategies, and product and segment characteristics to those in product development, and behavioral and motivational issues to those trying to capture consumers' attention.

Developing a highly acceptable product and marketing it effectively involves creation of an inventory of lifestyles at different lifestages. Various methodologies are used to create a lifestyle inventory. An analysis is made of the factors affecting the lifestyle, and these factors are used to develop homogenous lifestyle groups. Lifestyle inventory helps in devising a suitable strategy and designing new products and services, suitable to the target groups.

Private banks have already adopted lifestyle-marketing strategy, which has prompted some of the public sector banks to rethink on their strategies and ways to blend their marketing effort towards lifestyle marketing strategy. Proactive approaches like studying evolving lifestyles can provide insights into the design of newer products suited to the evolving lifestyles. This would, of course, require more data about the customers.

Source: ICFAI Research Center.

E-BANKING – AN INTRODUCTION

Before the advent of the Internet, Electronic banking has existed for around two decades, but it was limited to direct-dial services. The increase in e-commerce has speeded up this process in recent years due to a rise in the use of Internet. Most of the banks are now offering electronic banking services with increasing competition from Internet-enabled, or online, banks and other financial organizations.

Both computer and telephone banking cover the term *electronic banking* or *e-banking*. Using computer banking, a customer's computer either dials directly into his bank's computer or gains access to the bank's computer over the internet. Using telephone banking, the customer can control his bank accounts by giving the bank instructions over the telephone. Both computer and telephone banking involve the use of passwords, which give access to the customers' accounts.

Banking transactions can be carried out 24 hours a day using these methods. For instance, a customer can view recent transactions, get print out of statements of account and transfer funds between accounts and make payments or transfer funds using computer banking. Many banks have provided the facility to set-up, amend or cancel standing orders.

Evolution of E-Banking

Banks and Financial Institutions are service-providing organizations, operating within a nation or across the word. They serve very large number of clients. These institutions provide service through a network of branches and cater to the needs of their customers in different areas with personalized service. Traditionally the manual processing of data applied "pen and ink" as tools and recording data in several ledgers, books and registers. They depended on newspaper and other media publicity for reaching their customers whenever any important message had to be conveyed on a mass scale. Manual service was cumbersome, slow and tardy. Customers had to wait in serpentine queues before the counters, extending these services, for their turn to be attended by the bank staff. They had to fill up multiple forms and other printed stationery needed by the service provider and had to remain at the premises of these Institutions for a considerably long duration to complete their transactions.

Similarly, transactions between sister branches of the same institution and the data transmission to the head office and other controlling offices, if any, were all done conventionally through manual process. The system was slow and tardy. It was costly, as the banks and other institutions had to engage a large array of clerical and supervisory manpower to carryout and later to check and re-check the accuracy of the tasks performed manually. Despite these elaborate steps, errors in calculations and wrong data copied or incorporated went undetected and posed serious problems at the time of reconciliation of the accounts.

The Advent of Technology

The developments in information technology, the advent of the personal computer and networking technology in the eighties brought about partial relief. The job at each seat was computerized by stand-alone personal computers initially. Errors in calculations and other types of data have reduced with this. Customers were provided error free service and were supplied with printed account statements. The enormous expansion of business in banking and financial institutions in the eighties would have caused operational breakdown but for this timely innovation in the work system. Still extensive manpower employment could not be dispensed with and overcrowding of customers at the counters of the banking and financial institutions continued.

It is in this context that Internet and the concept of e-commerce entered the scenario of global banking and financial institutions. Simultaneously sweeping structural and functional changes are overtaking the International banking and financial markets. These changes are described here under.

Deregulation

Growing deregulation in national financial markets and the revolution in telecommunication and data processing technologies resulted in the better integration of financial markets in all countries as also between the domestic financial system and the foreign banking and non-banking institutions.

The conservative era, in which the banks were prohibited from venturing into any field other than traditional banking, gave way to a liberalized thinking that banks should be permitted to sell products hitherto barred to them such as retail lending, loans against property, selling insurance products and mutual funds. Thus, the concept of Universal Banking came into the picture.

Owing to growing international commerce and economic development there was an explosion in the growth and turnover of transactions and number of clientele for the banks.

The catalytic agents that enabled all these metamorphosis in banking and financial services include: the advent of the fourth generation personal computers, development of Internet and networking technology as also the advancement in telecommunication facilities. Global players like Citibank and GE Capital are now able to reach a vast number of clientele spread geographically in different areas through limited branches they have set-up, by skillfully reaping the benefits of Internet banking and e-commerce.

Box 3: Internet – E-Commerce – E-Banking

Internet brought unprecedented changes in the society. The Net has redefined the methods of communication, work processes, study, education, interaction, entertainment, health, trade and commerce. It has offered interesting services like e-mail, e-commerce, file retrieval and other Internet tools. It has an immense influence on every aspect of our lives.

The versatile facilities and opportunities provided by the Internet and World Wide Web led to the development of electronic commerce. This became possible when the Internet transformed from the original system of providing static web pages, into an interactive two-way medium due to the advancement in software technology. Electronic Commerce is a system, which includes transactions that center on buying and selling goods and services directly to generate revenue. Electronic commerce builds on the advantages and structures of traditional commerce by adding the flexibility offered by electronic networks. E-commerce helps conduct traditional commerce in new ways, and transfer and process information which is at the heart of commercial activity.

Source: ICFAI Research Center.

Security Solutions

E-banking and electronic financial services are branches of electronic-commerce. The primary problem faced by both service providers and seekers through the electronic media at the earlier stages was security, integrity of the transmitted and stored data, and unscrupulous hackers interfering and manipulating transactions. They could intercept messages from the electronic media, and get access to sensitive data like “passwords” and credit card numbers and thereafter extensively hack the websites. Extensive cases of “computer-crimes” and “computer-frauds” happened in the initial stages.

But, as we know, every necessity serves as the mother of a new innovation and invention. Software engineers developing new devices like Site Security Firewalls, Filtering Routers, Secured Socket layer, 128-bit encryption environment, Verisign Digital Certification and so on quickly tackled the problem.

A dedicated system designed to provide a layer of security between corporate systems and the public Internet is called as firewall. Incoming network connections can be prohibited, selectively or totally, making it possible for users to dial out but impossible for others to dial in.

Based on predefined rules a router can filter packets of information. Secured Socket Layer or SSL protocol provides browsers and web-servers with three important security services – encryption, certificates and message integrity. Integrity is the mathematical way of checking if the message received by the browser or server has been tampered with. The risk of unauthorised persons reading the user's data as it travels across the net is solved by Encryption. The encrypted data is scrambled so that unauthorised persons do not understand it even if they access it. In electronic transactions the user can encrypt a digest with a private key to create a digital signature. These innovations cleared the barriers for the fast development of all facets of electronic commerce.

Availability of Software

Internet and World Wide Web have come to be extensively used in banking transactions in a number of ways. This has provided immense benefit to the customers, and ensured total accuracy of transactions. Banks are able to provide services to the customers for 24 hours per day and 7 days per week, otherwise known as any time-any where banking, without the customer visiting the banks premises. Specialized software, developed by technology firms, was suitable for use by banks and financial institutions and many new products came into usage. Banks and financial institutions have benefited on the following counts:

i. Hosting their website on the World Wide Web to publish their corporate image on the global level and furnish detailed information about the products, services they offer, as also the terms and conditions thereof. If today one wants to know about some service offered by American Express or Citibank or Standard Chartered Bank, one need not visit these institutions or seek information over the phone, the person can simply surf their respective web pages on the Internet. In case the person desires to know some information over and above what has been stated on the website, he/she can get the same through an e-mail.

ii. Total elimination of manual processing of data in terms of internal routine like inter-branch reconciliation, monthly salary processing, posting and finalization of financial accounts and annual statements consolidating the transactions distributed at several centers etc., resulted in productivity improvements in leaps and bounds. The tasks which were earlier handled by 10,000 workers can now be performed by a mere 500 to a maximum of 1000 workers. All that the human worker has to do is to input the primary data from control records to generate vouchers, subsequent processes are automated. The bank employee was outside the realm of business policy and planning, and attending to simple clerical processing, now has become a knowledge worker, who is no longer bored with monotonous repetitive figure-calculations and duplication of records.

iii. Selling products to individual customers (B2C commerce) and to corporate customers (B2B Commerce) by banks, insurance companies, stockbrokers, mutual funds etc.

Thus, the World Wide Web has provided the most convenient means for universal communications. Banks and Financial Institutions host their websites on the web and provide information about their profile, about the key persons in the

management, their products and services, and rules and terms of service. No length of newspaper advertisements or other media publicity can surpass this mode of information transmission, since the sites are indexed through search directories. Even a person who has no inkling of the particular bank or institution will gain access to the information, when he/she searches the appropriate subject.

Use of Intranet

Large organizations that employ thousands of persons and operate over wide geographical area develop enormous internal routine and administrative systems and procedures. Much of this data can be computerized at a single location, and the task of integration of the data from units of the organization is achieved by linking the networks of different branches/geographical units through an Intranet. An Intranet is a wide area network and works on the same methodology as the Internet, but it is restricted to specific users or institutions and external access is not allowed. The head office or administrative offices are thus linked to the systems of the branches through the Intranet. Using intranet, MIS returns for any branches can be directly compiled at the administrative office or Head office, which also solves the recurring problem of reconciliation of inter-branch accounts.

Types of Electronic Banking

There are two types of banks that offer electronic banking services: the traditional high street bank and the Internet-only bank.

TRADITIONAL HIGH STREET BANK

Many high street banks are now offering electronic banking services for business customers as an alternative to, or to complement traditional branch banking. Some of the traditional high street banks are: SBI, HSBC and Syndicate Bank. But, they also started providing e-banking services partially. They are providing two different methods of connection to the customer's account, viz., Direct-dial/PC banking and Web-based Internet banking.

Direct-dial/PC banking: Direct-dial works via a dedicated phone number when the customer dials directly into the bank's server. With direct-dial, customers need to use customized software provided by the bank itself. This allows the customer to download their account details from the bank's network and view them offline.

Web-based Internet banking: Web-based Internet banking involves a customer logging onto a bank's online banking services via any compatible PC to perform common banking transactions.

INTERNET-ONLY BANK

A number of banks have no branch network and are exclusive to the Internet. Some of the Internet-only banks are: Griffon Bank, Zions Bank, Compubank, Swissquote Bank and first-e. Internet banks usually offer a number of services in addition to regular bank accounts, from credit cards and loans to insurance and investments. Such banks tend to offer better rates and deals than regular high street banks, simply because they can. An Internet bank is a lot less expensive to run than a high street operation, and is therefore able to pass these savings on to its customers through cheap loans and higher interest rates on savings.

The Internet Bank system allows the customers to manage and monitor their accounts online and to use the full range of electronic banking services from anywhere in the world using a personal computer. A customer needs a connection to the Internet and a browser such as Microsoft Internet Explorer or Netscape Navigator to use the Internet Bank system. A very high level of security, such as 128-bit encryption, is established for Internet Bank systems. A customer needs to have Internet bank login and password to log onto the Internet Bank and his/her Digital Signature is needed to confirm each electronic banking transaction.

Services on Offer

The Internet-only banks offer a range of services, some of which are similar to those offered by traditional banking methods in the high street branch, that include:

- Viewing account balances and recent transactions.
- Paying bills to utilities companies and suppliers etc, without having to write cheques.
- Scheduling bill payments in advance.
- Transferring money between the business' accounts.
- Setting up and checking direct debits.
- Setting up and making direct payments to other banks and building societies.
- Viewing the bank statement.
- Viewing, activating or canceling standing order details.
- Sending messages to the bank via e-mail.
- ATM access.
- Debit and checking cards.
- Download ability into Microsoft Money or Quicken applications.
- Instant account updates.
- Interest bearing checking, savings and money-market accounts with 24-hour online access.
- Mortgage and home equity loans.
- Online check ordering and direct-deposit set-up.
- Overdraft protection and line of credit.
- Small business services.
- Stock quotes and trading.

Setting Up a Bank Account

To bank online, certain hardware and software will be required. The hardware required will be any IBM-compatible PC, with Windows 95 or later operating system and latest versions of Microsoft Internet Explorer or Netscape Navigator web browsers. In addition, a modem of at least 28,000 kbps and a telephone or cable connection will be needed.

The registration process varies from bank to bank. Some allow registration only by post, some provide registration online and some a combination of the two. Certain common sections such as personal details, the business name, type and number of employees, the organization's address, the branch sort code and the account number are however, need to be completed. For many banks the applicant has to be an existing branch customer to sign up for online services although this is not always the case. The number of authorized signatures required depends on whether the business is a sole trader, partnership or limited company. When is a joint account; at least two parties need to sign the account mandate. In cases where access is given to a third party, authorization needs to be given by the account-holding customer and by the branch. The account holder(s) need to agree to the bank's terms and conditions by signing and returning the form. A short delay of about five days ensues during which the bank verifies the signature(s) against its branch's records. Finally, a mailer is sent out to the customer, which contains a user ID and an online password. In the case of direct-dial, the software and PIN (Personal Identification Number) are included.

Costs

The costs of electronic banking vary from bank to bank. Some offer completely free electronic banking services while others charge a one-time set-up fee in addition to a monthly fee and normal transaction charges. Some banks are reducing costs for customers by entering into joint ventures with existing Internet Service Providers (ISPs) and are therefore able to offer free Internet access. Electronic banking is in fact mutually beneficial to the bank and to the customer. From the bank's point of view, it requires fewer staff members and reduced overheads; while for the customer, it is considerably cheaper, compared to traditional banking services, with lower charges and increased interest rates.

Security Measures

Much of the media attention is focused on security aspects of electronic banking. It is only natural that business customers should show concern about sending their personal details and account numbers over the Internet. However, in reality it is no more risky than giving credit card details over the phone or paying for goods/services with a credit card at shops/restaurants. The security measures of electronic banking can be implemented partly by the bank, through its security systems, and partly by the business customers themselves, through their own vigilance. Security operates at three different levels.

BANK'S SECURITY

The data exchanged between the bank and the customer is coded or encrypted. Most banks use secure servers, with 40 bit SSL servers (Secure Sockets Layer), which sit behind firewalls and 128-bit encryption. More recent web browser software ensures a higher level of encryption. The likelihood of a computer hacker breaking through these security measures is very unlikely.

ACCESS SECURITY

On registration, the account holder submits a piece of personal information of his choice from a list of five, for example, the name of his first school, and a memorable date other than the account holder's birthday in case he needs to call the customer helpline. Normally, two levels of security are used each time the customer accesses his account details: a user ID and password.

ACCOUNT HOLDER'S VIGILANCE

However tight the bank security systems are, it is not sufficient. Customers need to play their part too and exercise caution when banking online. Security measures include:

a. Not divulging their PIN number or password to any third party.

b. Not leaving their PIN number anywhere around.

c. Not leaving their PC while still being logged on to the bank website. The customer should not rely on the online bank website to automatically time out.

d. Making sure nobody can see the details on the computer screen or ensuring that the equipment will not allow electronic eaves-dropping.

e. Not sending e-mails containing their password or membership number.

f. Always removing any data that has been exported to a financial management package.

g. Taking note when the PC/Internet screen indicates whether the customer is operating in a secure environment.

ADVANTAGES

Banks are realizing that they need to do more than just offer traditional services on a flashy web page. Those who are serious about succeeding in cyberspace are broadening services and reducing consumer costs. They are also offering personalized experiences and customized interactions.

Cost Effectiveness

Many banks offer favorable interest rates and low charges when using electronic banking. The small business can avoid costly cheque fees by transferring payments electronically to its suppliers, employees, telephone and utility companies. The only cost incurred will be the price of a phone call. Even then, some Internet Service Providers (ISPs) are now offering subsidized Internet access–so phone calls may be cheaper.

Cash Flow

With electronic banking, business customers can regularly monitor their cash flow. Overdraft charges on a current account can be reduced by transferring money between accounts. Excess cash may be kept in high-interest bearing accounts and easily moved to the current account to make external payments. The customer can view all the accounts' balances up to the end of the previous day. On the basis of this information, informed business decisions can be made while avoiding unnecessary financial risks.

Convenience

At any time of the day or night accounts can be accessed online. There is no need to travel to the nearest bank branch, nor rely on their limited opening times. Web-based Internet banking services aim to offer 24 hours a day, 7 days a week service availability.

Time-saving

When a business customer used the internet banking he/she can avoid spending time on the phone or waiting in a queuing system to speak to a bank representative.

DISADVANTAGES

The disadvantages of electronic banking include:

Internet Connection Speeds

Connections to the Internet and server can sometimes be slow. This is particularly true during the busy times of the day, for example, such as in the morning and late in the afternoon. At worst, a customer could spend more time online than would be spent on the phone.

Extra Staff

A small business may need to employ an extra member of staff to have sole responsibility for conducting the business's financial affairs via the bank's electronic banking services. Without this extra member of staff, the owner or manager may be detracted from running core business activities and making key business decisions.

Security

Because it is not conducted over the Internet but via a dedicated phone number, direct-dial banking is inherently more secure than Internet banking. Security issues are covered in detail in a later chapter of this book.

E-Banking and Corporate Clients

Traditionally, business bank accounts were underpinned by a solid relationship between the bank manager, who used to be in the same job and branch for years, and the business owner. This model drastically has been changed by restructuring and reorganizing of banks branches.

What matters to the business owner today is less the opportunity to play golf with his local bank manager and more the chance to access consistent, reliable, high-quality

advice swiftly; the ability to check balances when he wants to; and processing cheques in an efficient way, paying suppliers and so on. As a result, today the clients/customers of many banks are able to have the e-banking facilities. Services offered by Indian banks include:

- Account Information: Real time balance information and summary of day's transaction.
- Request: Make a banking request online.
- Account Information: The complete database that the bank has about a company is available at the terminal;
  - Current balance in the company's account on real time basis
  - Day's transactions in the account
  - Details of cash credit limit, drawing power, amount utilized, etc.
- Downloading the account statements as an excel or text file. The statements can be integrated with the ERP system for automatic reconciliation.
- Fund Transfers: One can manage Supply-Chain network effectively by using online fund transfer mechanism. The fund transfer takes place on a real time basis across the bank locations. This product facilitates
  - One-to-one fund transfer between two linked accounts.
  - Bulk fund transfers. In bulk fund transfers, you upload a flat file containing payment/collection information. Some of the banks' systems take care of processing the entire file, and once the file is processed you can integrate the processed file to your ERP for auto reconciliation.

The real life situation of user-wise limits and multilevel signatories can be mapped in the net-based fund transfer. You can specify user-wise cap for funds transfer and the number of approvals needed for each fund transfer. The fund transfer will not take place unless the required number of signatories has approved it.

With a Power of Attorney from the suppliers/dealers, one can link the dealer's accounts to his/her account in order to have an online fund transfer, saving time and money involved in cheque collection systems. Alternatively, the dealer can credit his/her account through this channel. Similarly, one could also effect vendor and other payments online.

Customers can also submit the following requests online:

- The account statements by e-mail either on daily/weekly/ fortnightly/monthly basis
- Stop payment of cheque
- Cheque book replenishment
- Demand Draft/Pay-order
- Fixed deposit account opening
- Opening of letter of credit.

Operation of Corporate Internet Banking: A registered user enters his *Corporate ID*, *Used ID* and *password* for accessing the facility. He can view all the accounts across all the bank's locations online and as well effect fund transfers on real time basis within the bank network. The fund transfers are stored in his database at the bank and are available to him later to integrate with his MIS.

The Security Features Embedded in the Software: Total security is ensured to prevent hacking at the site through foolproof devices. Precautions in terms of firewalls, data encryption, and digital certification provide total security and prevent hacking at the site so that no malicious or unauthenticated person will be able to access the customers' database. Other features include a safe password that

only the particular customer or the authorized persons in the customer's organization will know, and even the bank employees will not have access to the customer's password. There will be no memory caches allowed on the navigator so that after the customer logs out another person will not be able to access the browsed pages by pressing the "Back" button on the navigator. Also there is a time out for the screens. It automatically logs the viewer out from the site if the screen is not used for defined number of minutes.

Benefits to the Customer: The company does not have to spend anything extra to avail such facilities. All it requires is Internet connectivity. The product enables the company to proactively manage its cash flows, ease reconciliation efforts, as all the MIS is available at the click of the mouse.

Integration with the Client's ERP System: The account statements of the customer can be downloaded either as a text file or as an excel file. The account statements and bulk payment files can be integrated with his ERP system with the help of the bank. The bank depending upon the nature of work involved may charge a nominal fee.

E-Banking and Individuals

Bill Payment through E-Banking

The concept of any time and anywhere banking has thus been ushered in by the Internet. The electronic Bill Pay service provided by the banks overcomes the individual's onerous task of visiting several places to pay his service bills like telephone, water and electricity. Right from his desktop he can pay his regular monthly bills such as telephone, electricity, mobile phone, insurance etc. No more missed deadlines, no more loss of interest – he can schedule his bills in advance, and thus avoid missing the bill deadlines as well as earn extra interest on his money.

The Electronic Shopping Mall

The customer can also make his shopping payment through the bank's secure website – so that he can shop online without any security worries, as the bank can provide online real time shopping mail services through partner shopping sites.

Effecting Personal Investments

The bank's website can also allow the customer to invest in shares, mutual funds and other financial products.

Trading in Shares: Cash Trading

This is a delivery based trading system that involves taking delivery of shares or monies.

Trading in Shares: Margin Trading

Customer can also do an intra-settlement trading normally up to 4 times his available funds, wherein he can take long buy/short sell positions in stocks with the intention of squaring off the position within the same settlement cycle.

Trading in Shares: Spot Trading

'Cash on Spot' may work the best for him, when looking at an immediate liquidity option. On selling shares through "cash on spot", money is credited to his bank account the same evening and not on the exchange payout date. This money can then be withdrawn from any of the bank's ATMs. The customer can also trade directly at the recognized stock exchanges of the country through his bank.

Investing in Mutual Funds

The same convenience while investing in mutual funds – hassle free and paperless investing is brought to the customer by electronic banking. He can invest in mutual funds without the hassles of filling application forms or any other paperwork. He needs to provide no signatures or proof of identity for investing.

Once he places a request for investing in a particular fund, there are no manual processes involved. His bank funds are automatically debited or credited while simultaneously crediting or debiting his unit holdings.

Trade in Derivatives: Futures

The customer can also do trading in index and stock futures on the approved stock exchange through electronic banking. In futures trading, he takes buy/sell positions in index or stock(s) contracts having a longer contract period of up to 3 months.

Trade in Derivatives: Options

An option is a contract, which gives the buyer the right to buy or sell shares at a specific price, on or before a specific date. For this, the buyer has to pay to the seller some money, which is called premium. There is no obligation on the buyer to complete the transaction if the price is not favorable to him.

He has to place certain percentage of order value as margin to take the buy/sell position on index/stock options. With options trading, he can leverage on his trading limit by taking buy/sell positions much more than what he could have taken in cash segment.

IPOs Online

Without going through the hassles of filling any application form or paperwork the customer could also invest in Initial Public Offers (IPOs) online. He can get in-depth analyses of new IPOs issues, which are about to hit the market. IPO calendar, recent IPO listings, prospectus/offer documents, and IPO analysis are few of the features, which help a customer to keep on top of the IPO markets.

Thus, the variety of services that can be provided through the electronic channel by banks and financial institutions is endless. To woo the customer, every institution is trying constantly to innovate and offer new products. The benefit to the customer on account of the Internet is that he is able to know at a time the types of facilities being provided by different institutions and he is able to make the best choice suited for his needs.

The benefits to the employee are equally amazing. From being a dumb worker filling up forms and copy from books, he is now a regular service provider and one who directly cares for the customer. Today he handles customer's demands whereas earlier he was dealing with a particular process. In turn the knowledge resources required of him have grown and he is able to secure the same through better training and other organizational development programs like work groups and functional teams, where persons with different skills and qualifications pool their knowledge and carry-out high-tech services and operations.

E-BANKING IN INDIA

The backbone of every country is the financial sector, comprising banks, stock exchanges and insurance organizations. It is instrumental in implementing and bringing about economic reforms. Any changes in this sector will have a sweeping impact on the country. The stock markets in the last decade; with the introduction of electronic trading, settlement and depository; have experienced a significant contribution from technology. The cost per transaction to the investors and other intermediaries in the market has come down significantly, besides bringing total transparency in market operations as a result of the introduction of automation in stock markets.

The reforms introduced in 1990s have initiated a healthy competition among the banks. As a result, they have started improving customer service and find technology to be an ideal tool to achieve this objective. In a manner, the banking and financial services sectors – being the early adopters of any new technology – defined the

roadmap for future technology adoption. Banks are now focusing on three core issues:

- How to meet customer's service expectations?
- How to cut costs?
- How to manage competition?

Information Technology (IT) is central to banking. It has moved from being just a business enabler to being a business driver. Technology can help banks in attaining their objectives. To achieve their goals banks are exploring new financial products and service options that would help them grow without losing existing customers. And any new financial product or service that a bank offers will be intrinsically related to technology.

Technology is the Key

Technology is the basic necessity that banks need to have in place, and it includes a combination of centralized networks, operations, and a core banking applications. Technology enables banks to offer services on a 24x7x365 basis, using lesser manpower.

However, banks need to think beyond just basic automation, to be really competitive. IT has changed the way a bank reaches out to its customers. Gone are the days where IT was deployed for automating accounting/back office functions to remove drudgery of employees. It is now massively being deployed for customer interfacing/interaction. A better way to understand the technologies that would define the future of banking would be to start in the past.

Evolution of Technology in Indian Banks

The Rangarajan Committee report in the early 1980s was the first step towards computerization of banks. Since then, banks have started exploring the idea of 'Total Bank Automation (TBA)'. Though titled as 'Total Bank Automation,' in most cases, it was confined to branch automation only.

It was not until 1990s that banks started thinking about tying-up disparate branches together to facilitate information sharing. At the same time, private banks entered the banking arena with radically different strategies. Given the huge IT budgets at their disposal and with almost no legacy IT equipment to worry about; private banks hastened the adoption of technology. Providing a whole new range of financial products and services at minimal costs was the philosophy with which private banks started their operations and the technology made this possible.

The improved connectivity, in terms of leased lines and VSATs, and falling costs provided a boost to inter-branch automation. It became more feasible for banks to network their branches with the help of improved services and lowered costs of service providers, such as DoT and VSNL. This gave banks an impetus to network all the branches and setup centralized databases. These developments made it possible to have operations such as MIS and to be truly automated and centralized.

With centralized infrastructure and numerous connectivity options, banks started exploring multiple delivery channels like ATM, Net-banking, mobile banking, and Tele-banking thus driving down cost per transaction. For retaining customers and lowering service costs to the customer, banks are increasingly adopting core-banking solutions.

Centralized Infrastructure

In the early days of banking technology, the network and backend infrastructure used to be decentralized. This meant that each branch had its own server(s), banking applications, database(s), and other such assorted hardware/software.

However, decentralized networks had their own set of problems in terms of the cost and management. The decentralized model involved huge capital expenditure and resources; there was no coordination or a central control point. They experienced problems while updating applications and troubleshooting, forcing the technology representatives to be present at each branch to provide support.

That was an acceptable scenario till the multi-channel facility came into the picture. These new concepts created the need for centralized databases. New delivery channels required that, irrespective of the branch or channel the customer used, the database be updated instantaneously. The networks had to be up and running and be managed with lesser costs. Although the data centers were being used by some of the banking majors, they were never considered as being capable of being a central hub of operations. Things changed when banks realized the costs and benefits of swapping the decentralized model to centralized datacenter architecture. Centralization, using a data centre, has helped a lot in improving and simplifying the network from the operations, user and administration perspectives. From a cost perspective, centralization has proved very effective.

It is not just the datacenter, which contributed to centralization. The network has also evolved into a unified IP network. Banking networks used to be a pot-pourri of several older protocols in olden days. There used to be one network for data traffic, another for telephony, and so on. Today, a single IP based network is used, irrespective of whether it is data, voice or videoconferencing, ATMs or mobile banking.

Core Banking Applications

After consolidating the databases and networks the banks have started focusing on core banking applications. Core banking applications help provide complete front and backend automation of banks. These applications also help banks achieve centralized processing and provide anywhere, anytime 24 x 7 non-stop services, which is not possible with traditional localized branch automation systems that are available only during their working hours. Core banking applications help integrate the enterprise to existing in-house applications to offer a single customer view. These applications provide automation across multiple delivery channels.

Now, banks are increasingly adopting core-banking solutions for retaining customers and lowering service costs to the customer. Banks are reinventing themselves as marketing agencies by selling products like life insurance, RBI bonds, credit cards, etc. The core banking applications are able to support all these activities.

Risk management is another area where core-banking applications are of great help to the banks. These systems take care of the risk monitoring and comply with the reporting requirements. In addition, loyalty programs can also be monitored and managed using a core banking application.

Focus on Customer Satisfaction

Managing customers is one of the main issues that banks face in today's hyper competitive environment. If the service levels are not up to customer expectations, in all likelihood the customer might take his business elsewhere. This is where Customer Relationship Management (CRM) practices and software play an important role.

Banks have started to know the customer better. They are able to assess how many customers have moved in the past and how existing customers are using various services that the bank provides. Such information is important because, in banking, being the first to market alone is not enough as products can be copied very fast. It is the customer service levels that matter.

This is where CRM techniques and tools come into play. While a foremost part of CRM strategy is all about treating the customer right, technology does make a major difference. CRM is a tool that allows the banker to emote and relate to the customers. Increasingly, all banks will require the CRM as they get centralized.

CRM TOOLS

CRM tools can be broadly classified into two categories: Operational and Analytical. Operational CRM tools provide the software support for businesses that require customer contact. These tools are largely workflow based; they provide information to employees and document customer interactions. This includes collaborative CRM type tools used to provide enterprise/customer interaction across all contact channels such as face-to-face, telephonic, electronic, and wireless. Operational CRM types are the major CRM tools being used nowadays for customer support in India. For example, when a premium customer dials a bank's call center from his home, the operational CRM can alert the call center executive of his account status and other details. This will help the employee in providing him the kind of service that is extended to a premium customer.

Analytical CRM helps a bank make sense out of the available information. It helps the bank target customers and utilize the potential to the maximum. For example, if there is an account holder, who withdraws Rs.10,000 every month from his account and deposits it in another bank as EMI for a loan. Analytical CRM tools can help the bank track this activity. Techniques such as data warehousing and data mining are prominent tools used for this. With this piece of information the bank could offer a loan to the customer at a lower rate than what the other bank offers. This will keep the customer happy, when he knows that you are providing him better services. Thus, it translates into the satisfied customers and improved profitability to the bank.

However, banks tend to forget an important aspect about CRM; the CRM is more than just a technology implementation, it has to be a clearly defined process with appropriate customer service levels. This is the reason why some CRM implementations result in limited success.

Box 4: Increasing Importance of CRM

Loyalty seems to be a thing of the past. Organizations are offering several incentives to maintain the customer loyalty as they have understood the need to put the customer at the center of their thinking. Now, CRM is the latest buzzword in banking industry. The banks are vying with each other in developing an ideal relationship model to acquire new customers, retain the old ones and to serve the existing as well as the prospective customers.

Banks have activated their data warehouse to conduct a more purposeful study into the behavioral patterns of their customers, so that they can develop new products as a result of such analysis. Data mining has emerged as an important tool for decision-making by the management. In addition, Executive Information Systems (EIS) and decision Support Systems (DSS) have become faster and more accurate as they are now able to use data mining. Firms in financial services industry have started investing in CRM technologies. Mass customization may be the challenge for the future customer relationship. However, the Internet is being used as a medium to interact with millions of customers on an individual basis. Some of the other means of interaction include customer relationship managers, field-level sales force, help desk, call centers, interactive voice response systems, kiosks, interactive television and e-mail.

Source: ICFAI Research Center.

Data Mining for Intelligence

Another important issue that the banks have to deal with is proper analysis of financial data to identify business potential. This will help a bank identify cross-sell and up-sell potentials. Again, technologies such as data warehousing and data mining assume an important role in this context.

A bank can easily streamline its delivery channels if it has an operational CRM. Further, if the bank's CRM is backed with data warehouse solution, it can streamline the channels and set direction to them. In other words, it tells them which customer to focus on. A data warehouse enables the bank get a single view of its data across disparate systems, which will be a great advantage to the banks as most of their data is spread over several disparate, including legacy, systems. If the data is spread across different systems, a transaction done on one system will not be reflected in the other, which is not a desirable phenomenon in the context of multi-channel banking.

Data warehousing offers a solution to the above problem by integrating all the data into a common warehouse (usually an RDBMS). The multiple data coming in from different systems is converted into a common format using the ETL (Extraction, Transformation, and Loading) process. The common format provides a single repository from which one can view or use information when required.

However with the data available in data warehouse one will not be able to make sense out of it, it requires data mining for the purpose. Data mining can help you recognize patterns in the available data. For instance, if a bank's manager is interested in knowing how many of its customers have monthly incomes exceeding Rs.15,000 and own a two wheeler, data mining can provide an answer. The answer to this question will give a list of prospective customers to whom the manager can offer a car loan. All that the manager needs to do is give the query to the data mining tool and it will provide him with the answer in a jiffy. Thus, data mining and data warehousing can help banks identify the right customer for a particular promotion. They also help in cross sell and up sell of services to customers.

INTERNET BANKING STRATEGY

Internet will radically alter the Banking and Finance industry. This will have a much larger business impact than ATMs and telephone banking. It will change the fundamental way of doing business as the capability exists for anyone, anywhere in the world to access his/her bank using a computer system run by anyone, anywhere in the world at a reasonable cost, with reasonable performance, and in a standard manner.

So far many banks are treating the Internet, specifically in terms of their Web presence, as just another element in the evolution of the delivery channel in the order of Branch-ATM-TelephoneBanking-HomeBanking-Internet. Though it is a logical assumption and to a certain extent true, it ignores certain implications by assuming that the Internet delivery channel is an adjunct to existing banking relationships and traditional delivery methods.

Having understood the importance of it some banks are setting up websites, and some are implementing Internet delivered transactions, though they still consider it as just another delivery channel. According to a survey conducted by Ernst and Young, 84% of banks are planning to offer PC based services, and 61% are piloting or planning Internet services. In this context the banks are slowly realizing that it is not just another delivery channel, it has more to it when we consider the following aspects:

a. Internet is growing exponentially

b. Most of the usage growth is in the most profitable customer segments.

The growth of Internet and its usage has been well documented. This growth shows no sign of slowing, and various developments such as the infamous "network computer" for turnkey Internet access, and the forthcoming delivery of Internet to the home via cable television and satellite broadcasting will provide additional impetus.

i. Today it is possible to build a bank based on Internet access; as a result of this non-bank competition will become an issue. Non-banks will be in a position to take the cream of the business, and leave the traditional banks and transaction processors with lower margins. Many non-banks are providing financial services and content today – software manufacturers, telecommunications providers, and information providers among them.

ii. Internet is a great leveler. With a relatively small investment, a small institution may build a very impressive Internet presence, offering excellent facilities, operating with a low overhead, no legacy branch network and much greater mobility. There will be little visible difference between large and small institutions. As the Internet based banking requires no investment in the delivery channel, and is largely a software-only investment, the entry cost to the Financial Services marketplace is much lower than before.

iii. The ease of Internet access offers much greater mobility and customers will be able to compare credit card rates, fees, lending rates and so on with immense ease, which puts greater pressure on operating margins.

iv. As a result of globalization the geographical boundaries are disappearing. It will be much easier for banks to participate outside their traditional geographical boundaries. Suddenly a bank may find out it has four hundred competitors instead of fourteen till the previous day. Some of the US resident discount financial service companies are planning and announcing to extend services via Internet to global customers.

The preceding discussion has demonstrated clearly that Internet can and will fundamentally change the banking business. If the banks, with their current key strengths, move quickly enough they can maximize their opportunities. Some of their strengths include:

- They have customer relationships, and can make the most of inertia of customer mobility, provided they can provide equivalent services.
- They enjoy the trust and a track record and a visible presence.
- They possess functional Call centers, ATM and Branch networks that will be valuable in the transition period.
- They have access to bank-only facilities such as SWIFT.

The Strategy

Firstly, the banks have to develop Internet presence and start building internal skills and infrastructure to support subsequent stages. This is a relatively low-cost exercise. The cost of one traditional branch will be more than that of the cost of setting up a fully functional Internet banking site. E-mail and web server capability is enough to start with. They should focus on critical factors such as bandwidth available and firewall/security issues.

They have to decide on the structure of the organization that will support Internet Banking activity. They should decide on the issues such as whether the new sew setup will be integral with the existing institution, a different branch or a different bank.

Then, they need to publicize e-mail contacts to customers so that the existing customers, who have e-mail capability and know-how, will be able to contact the bank using this medium.

It is important to publicize the web presence through the major and minor search engines. It must be made sure that any Internet user who uses a search engine and enters keywords such as "Bank" or the institution's name should be able to find the bank's website. It is extremely important not to underestimate the importance of dedicating resource to establishing 'web publicity'. New mechanisms for this are appearing literally daily, and it takes a considerable amount of effort to keep up with the developments.

The content of the website should carefully profile the customers of the bank that will use this media, and keep monitoring it. To begin with it will be typically business users and the more sophisticated personal customers. The bank should tailor the services to meet these segments. Provision of actual transactions requires careful planning and the security implications are fraught with problems, as with any online service, such as the method to be used to positively identify the customer with enough confidence to execute a financial transaction. However, these problems are not intractable. Of the many methods available today there are some that are workable without excessive complication of the user interface.

The banks can also consider co-operative marketing agreements with major business customers – providing links to their websites, or hosting websites on their behalf. Services such as travel products, insurance and so on lend themselves to web delivery.

For instance, assume that a bank has a corporate customer who is a car dealer. He can publish new car data, current prices and stock levels, colors and so on on the website. A customer can select the model, options and color, and receive a price and delivery time, and can secure the financing, through the bank, and complete the credit application. All that he is required to do is to walk in, sign, and take delivery of the car. This mechanism works for most of the goods, and it is even easier for lower value items where the payment can be made by debit or credit cards.

A bank can also consider a corporate payments terminal, delivered across the Internet, using a specific application at the customer end, supplied by the bank, to handle EDI, payments and account management in a secure environment, i.e., using the Internet as a neutral transport mechanism only.

When the banks facilitate usage of their services by customers in different countries, they need to provide multi-currency accounts and cards, denominated in the major currencies, which should be backed by electronic, real time, multi currency account to account transfer capability.

They can also consider developing, in conjunction with credit card companies, 'Internet only' payment tokens, such as credit cards without physical plastic, enabled for Internet payment capability only.

INTERNAL DEVELOPMENTS AND THE INTRANET

Banks spend lot of money on systems, systems infrastructure and IT staff. They almost always have a development backlog, and anything that can be done to help this has to be worthy of a look. Use of Intranet technology is the way to go.

Delivery of documentation, procedures, internal manuals and other material via an Intranet is both simple and cheap. Web servers can run on almost any platform, from mainframes to small PCs, and browsers with a common interface are available for almost any workstation. Training users on the use of an Intranet is simple and cheap.

In addition, if one examines the information requirements of bank personnel, and the system requirements for platform automation and an Internet banking system, there is a lot of commonality. This means that data published on the Internet website, such as product and service information, terms and conditions for credit cards, rates, loan modeling etc, can be copied with out reformatting to an internal Intranet for bank staff use.

For every system about to be developed, one has to consider whether all or part of it could be delivered using Intranet, and how much commonality there is with other web-based deliverables. The results are surprising, especially if the basic web functionality is enhanced by the use of languages such as, Java.

RISKS IN E-BANKING

The innovations in information technology and telecommunications had significantly transformed banking services relating to new product development, speed of transaction processing and reduction in transaction costs. It compels banks to offer a broad range of deposits, expand the geographical reach through new market penetration, and introduce credit and investment products through diverse distribution channels.

However, despite its advantages, there are inherent risk factors that accompany the introduction of high-tech electronic delivery system in the banking sector. Reliance on such technology often exacerbates traditional risks such as operational hazards, reputational and legal risks besides other risks related to business and credit offerings.

Transactions in e-banking may result in the 'digital divide' in terms of the access to banking services. E-banking and other IT-related innovations in the financial sector are knowledge intensive and they tend to favour the more educated participants, at the cost of ignoring the relatively less privileged sections. E-banking is vulnerable to various attacks and misuses. Unless, proper systems are in place banks will always be exposed to these risks. Security concerns in e-banking are fully addressed in Chapter IX of this book.

WHAT IS AHEAD?

So far we have seen the impact of information technology on various sectors of an economy, with special reference to banking sector. In the process we have noted the factors behind the evolution of e-banking and the current status and strategies to be adopted.

In the chapters ahead we will introduce the basic concepts of computers, networking fundamentals, enterprise computing and customer relationship management, evolution of computerization in Indian banking sector, risks associated with e-banking and the future trends of IT in banking.

SUMMARY

- Technology is a very dynamic force. It is changing the competitive landscape of the financial services and banking industry and is influencing the way their products and services are sold and delivered. There is an impact of IT on variety of sectors in the economy as a whole; these include business, industry, education, medicine and health care, government, defense services, security, management organizations, individuals and economy and individuals.
- With the advent of online transactions, speedy and secure settlement of payments has lead to the globalization of financial services. Better customer service is provided using various IT aided developments such as introduction of ATM, Magnetic Ink Character Recognition (MICR) cheques, credit cards, debit cards, smart cards, digital e-cash and electronic funds transfer. These

developments have helped in reducing the time processing transactions and also the services are made available to the customer at a convenient place. The day-to-day transactions in banks and insurance companies are automated which provide better service in processing transactions. Throughout the world, financial service providers are looking towards a new concept of 'anytime, anywhere, anyhow' banking.

- The term *electronic banking* or *e-banking* covers both computer and telephone banking. Both computer and telephone banking involve the use of passwords, which give access to the customers' accounts. There are two types of banks that offer electronic banking services: the traditional high street bank and the Internet-only bank. A number of banks exist that have no branch network and are exclusive to the Internet. This is called as Internet only banking. The Internet only banks offer a wide range of services as compared to traditional bank. The customer can avail several benefits from e-banking. In electronic banking, security is a major concern, hence security measures can be implemented partly by the bank and partly by the customers themselves.
- The Rangarajan Committee report in early 1980s was the first step towards computerization of banks in India. However, it was only in the early 1990s that banks started thinking about tying-up disparate branches together to facilitate information sharing. The improved connectivity and falling costs offered by leased lines and VSATs provided a boost to inter-branch automation. Banks are now reinventing themselves as marketing agencies by selling products like life insurance, RBI bonds, credit cards, etc.
- Managing customers is one of the main issues that banks face in today's hyper competitive environment. This is where CRM techniques and tools come into place. CRM tools can be broadly classified into two categories: Operational and Analytical. Operational CRM provides the software support for businesses that require customer contact. Analytical CRM helps a bank make sense of the information.
- A data warehouse can help the bank get a single view of its data across disparate systems. This comes in handy since most banks have data spread over several disparate, sometimes legacy systems. If the data is spread across different systems, a transaction done on one system will not be reflected in the other. This is not a very desirable situation when it comes to multi-channel banking. Data warehousing solves these by integrating all the data into a common warehouse. Data mining can help you recognize patterns in the data you have.
- Up until now, many banks are treating the as just another element in the evolution of the delivery channel. Firstly, the banks have to develop an Internet presence, and start building internal skills and infrastructure to support subsequent stages. Provision of actual transactions requires careful planning and the security implications are fraught with problems, as with any online service, such as the method to be used to positively identify the customer with enough confidence to execute a financial transaction.
- To facilitate usage by customers in different countries, provide multi-currency accounts and cards, denominated in the major currencies. Back this up with electronic, real time, multi currency account to account transfer capability. For every system about to be developed, consider whether all or part of it could be delivered using Intranet, and how much commonality there is with other Web based deliverables.

Chapter IV

Security Considerations in E-Banking

After reading this chapter, you will be conversant with:

- The Need for Security
- Sources and Types of Risks
- Causes of Risks
- Control Measures at System Level and Network Level
- Disaster Recovery and Contingency Plans
- Legal Aspects and Framework
- Security Policy

NEED FOR SECURITY

The growth in use of the Internet, most notably, the explosion in computer interconnectivity, has revolutionized the way the organizations and people around the world communicate and conduct business. The benefits have been enormous. A vast amount of information is now literally at our fingertips. Financial and other business transactions can be executed almost instantaneously, often on a 24 hour a day basis. Communication is quick and easy with unlimited number of other individuals and groups with the help of electronic mail, websites, and computer bulletin boards.

Computers have taken over virtually all of our major record-keeping functions. Recently, personal computers have made it cost-effective to automate many office functions. Organizations have begun to share data across wide areas. This has prompted efforts to convert principally LAN-based protocols into WAN-friendly protocols. The result has spawned an entire industry of consultants who know how to manipulate routers, gateways and networks to force principally broadcast protocols across point-to-point links, which are two different methods of transmitting packets across networks. Frequently the protocol of choice has been TCP/IP, which is also the primary protocol used on the Internet. To interconnect with each other via private networks as well as through public networks companies use TCP/IP. This presents ample scope to business organizations, governments and individuals to communicate with each other across the world.

Computerization has many advantages and it is here to stay. Automated systems, however, introduce new risks. Enormous risks to the computer systems, to the critical operations and infrastructures that they support, such as telecommunications, power distribution, national defense, law enforcement, financial services, government services, and emergency services follow the benefits of this interconnectivity. Now, we should be concerned with the risks that existed when manual procedures were used, as well as some new risks created by the unique nature of computers themselves. A malfunctioning sprinkler system in the computer room, an earthquake measuring 6.0 on the Richter scale, a disgruntled employee, or a misguided big cheese can do equal amounts of damage.

The Way Networks are Affected

Problems affecting one system will also affect other inter-connected systems. If not properly secured massive computer networks provide pathways among systems that can be used to gain unauthorized access to data and operations from remote locations. When businesses send private information across the net, they place a high value on it getting to its destination intact and without being intercepted by someone other than the intended recipient. Individuals sending private communications obviously desire secure communications.

The system itself can open up to attacks when connected to a network. The risk of data loss is high if a system's security is compromised. A great risk is posed when tremendous amounts of data is concentrated in one location. Greater the concentration of data, the greater will be the consequences of loss or damage.

Another risk is that computer users access information from remote terminals. We must be able to positively identify the user, as well as ensure that the user is only able to access information and functions that have been authorized.

User X transmits a file to user Y. The file contains sensitive information (for example, payroll records) that is to be protected from disclosure. User Z, who is not authorized to read the file, is able to capture a copy and monitor the broadcasts of the file during its transmission. These are some very simple examples.

The causes of risks and the likely effect they cast, the control measures to be adopted, and the approaches to evaluate them are discussed at length in this chapter. It also discusses security control measures and the legal aspects.

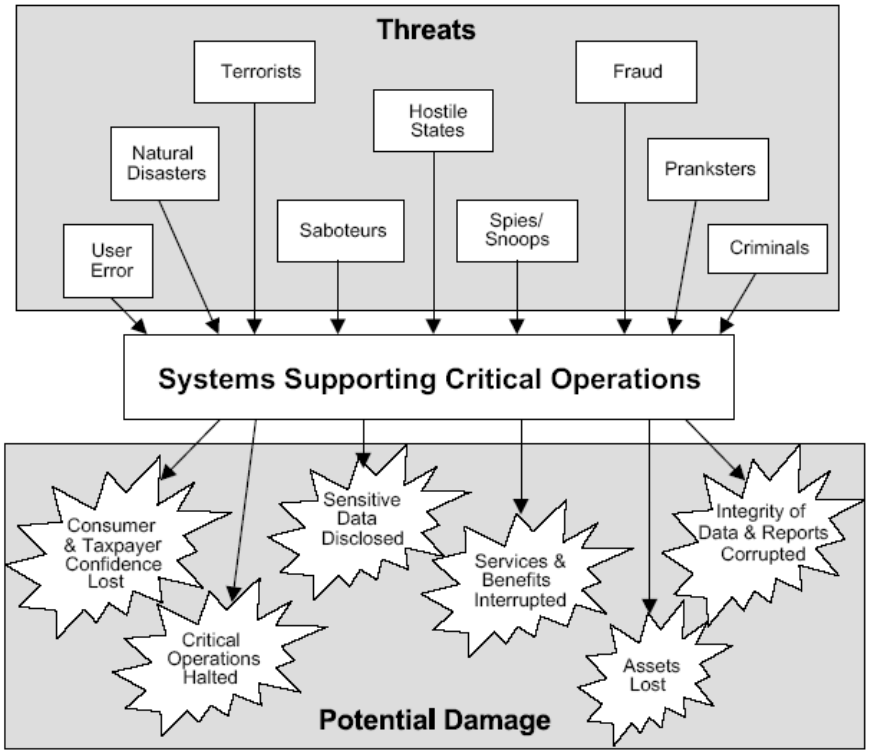
Components of Network Systems

All systems consist of three components: the software and hardware, the people, and the procedures. The same is true of computer and network systems. Security of the software and hardware, trustworthiness of the people who use and manage it, and reliability of the procedures for using and managing the system are the means of securing a computer system. Malice, ignorance, and acts of god or nature are the three kinds of threats to a system.

No matter what the level of technology upgradation risks of errors and fraud are the prime elements that influence and threaten the banking sector. But again, technology gains an upper hand and makes an effort to maintain these risks under control. Thus, only when it is able to control and prevent the risks to the maximum extent possible we can declare a system as being successful.

Due to customer demands, the banks and financial institutions are under intense competition. They are trying to provide customers with innovative products at lower costs and better services. Thus the quality of information that is contained in the communication networks and their application to the evolving business and customer needs measures the productivity of a bank. However, the risks associated in use of IT and deficiencies in security and controls within the banking procedures may pose a significant threat to the banking operations. Due to severe increase of dependence on the computers and IT related tools, the risks have not only extended beyond the traditional areas but have also become a vital reason of concern.

Figure 1: Risks to Computer-Based Operations



Source: Critical Infrastructure Protection, Comprehensive Strategy Can Draw on Year 2000 Experiences – Report to the Chairman, Special Committee on the Year 2000 Technology Problem, US Senate United States General Accounting Office – October 1999.

The risks discussed so far are not only specific to the banking sector but are encountered in all types of businesses.[1] The common effects of the risks are:

- Privacy violation,
- Setback of business due to improper decision-making,
- Financial loss due to computer frauds,
- Interruption in activities due to loss of data, hardware, software, people ware.

Risk, Threat and Vulnerability

The network's risk, threat, and vulnerability should be analyzed completely to assess in detail the requirements of your own network. First we will define the words *risk*, *threat* and *vulnerability*.

RISK

The risk is the possibility that an intruder may be successful in attempting to access your local-area network via your wide-area network connectivity. There are many possible effects of such an occurrence. Illegal access to information can result in disclosure, obliteration, or alteration of that information. In other words, it occurs when information systems are used or accessed for illegal purposes or for purposes they're not supposed to be used for. In general, the possibility exists for someone to:

- *Read Access:* Read or copy information from your network.
- *Write Access:* Write to or destroy data on your network (including planting Trojan horses, viruses, and back-doors).
- *Denial of Service (DoS):* Deny normal use of your network resources by consuming all of your bandwidth, CPU, or memory.

THREAT

The threat is posed when anyone with the motivation, attempts to gain unauthorized access to a network or anyone has authorized access to your network. Therefore, it is possible that the threat can be from anyone. A network's vulnerability to the threat depends on several factors such as:

- *Motivation*: How useful the access to or destruction of your network might be to someone.
- *Trust*: How well you can trust your authorized users and/or how well trained are your users to understand what is acceptable use of the network and what is not acceptable use, including the consequences of unacceptable use.

Types of Threats

The threats come in the form of viruses or take different other forms such as malicious programs, trap doors, logic bomb, Trojan horses.

- *Malicious programs:* These can be classified into two categories – those that need a host program, and those that are independent. The former are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program. The latter are self-contained programs that can be scheduled and run by the operating system.
- *Trap doors:* A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. They become threats when they are used by unscrupulous programmers to gain unauthorized access.
- *Logic bombs:* The logic bomb is a code embedded in some legitimate program that is set to 'explode' when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.

1 For a detailed discussion on various risks faced by banks, see Appendix I at the end of this chapter.

- *Trojan horses:* A Trojan horse is a useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function. Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
- *Worms:* Network worm programs use network connections to spread from system to system. Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.
- *Bacteria:* Bacteria are programs that do not explicitly damage any files. Their sole purpose is to replicate themselves. Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory or disk space, denying users access to those resources.
- *Viruses:* A virus is a program that can 'infect' other programs by modifying them; the modification includes a copy of the virus program, which can then go to infect other programs. A virus can do everything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs. The following are the most significant types of viruses:
  - *Parasitic virus:* The traditional and still most common form of virus. A parasitic virus attaches to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
  - *Memory-resident virus:* Lodges in main memory as a part of a resident system program. From that point on, the virus infects every program that the system executes.
  - *Boot sector virus:* Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
  - *Stealth virus:* A form of virus explicitly designed to hide itself from detection by antiviral software.
  - *Polymorphic virus:* A virus that mutates with every infection, making detection by the 'signature' of the virus impossible.

Box 1: New Virus Targets Banks!

A German Federal Office for Security in Information Technology (BSI) has alerted computer users of a new virus, which exploits security loopholes in the Windows OS and attacks online bank accounts and transactions made by credit cards on the Web.

According to the BSI alert, the new Korgo virus, which is similar to the Sasser worm that disabled millions of systems across the globe, can attack anyone connected to the Internet and primarily seeks out online banking passwords and credit card numbers. It does not require users to open an email to unleash its destructive capability.

Affected users are advised to change all passwords for online banking transactions and apply for new credit cards.

According to an Independent Online report, which quotes BSI, the virus has attacked Microsoft operating systems including Windows 98, Me, NT 2000 and XP. Microsoft has uploaded protection "patches" to shield computers against Korgo, the BSI said.

The best defenses against Korgo strains are updated virus definitions and the latest Windows patches from Microsoft, which can be obtained from windowsupdate.microsoft.com.

Source: http://resourcecenter.indiatimes.com/articleshow/748572.cms

During its lifetime, a typical virus goes through the following four stages:

- *Dormant phase:* The virus is idle. It will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses pass through this stage.
- *Propagation phase:* The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- *Triggering phase:* The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times this copy of the virus has made copies of itself.
- *Execution phase:* At this stage the virus performs the function, which may be harmless, such as a message on the screen, or harmful, such as the destruction of programs and data files.

Most viruses carry-out their work in a manner that is specific to a particular operating system and, in some cases, specific to a particular hardware platform. Thus, they are designed to take advantage of the details and weaknesses of particular systems.

VULNERABILITY

Vulnerability essentially is a definition of how well protected your network is from someone outside of your network that attempts to gain access to it; and how well protected your network is from someone within your network intentionally or accidentally giving away access or otherwise damaging the network.

Motivation and Trust: These are the two parts that you will need to assess in your own internal audit of security requirements and policy.

TYPES OF NETWORK RISKS

Denial of Service

DoS attacks are probably the nastiest, and most difficult to address, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.

The premise of a DoS attack is simple: Send more requests to the machine than it can handle. Toolkits are available that make this a simple matter of running a program and telling it which host to blast with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (hits on the website running there, for example). Such attacks were fairly common in late 1996 and early 1997, but are now becoming less popular. Preventive measures to reduce the risk of being stung by a denial of service attack include:

- Not running the visible-to-the-world servers at a level too close to capacity.
- Using packet filtering to prevent obviously forged packets from entering into your network address space.
- Keeping security-related patches for your hosts' operating systems up to date.

Unauthorized Access

A very high-level term that can refer to a number of different sorts of attacks is unauthorized access. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

Executing Commands Illicitly

It's obviously undesirable, to be able to execute commands on your server machines by an unknown and untrusted person. There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs. On the other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in place to cause the machine to shut down every time it's started, or something similar). In this case, the attacker will need to gain administrator privileges on the host.

Confidentiality Breaches

The threat model needs to be examined: what is it that you're trying to protect yourself against? There could be certain information that might prove quite damaging if it fell into the hands of a competitor, an enemy, or the public. It's possible in such cases, that compromise of a normal user's account on the machine can be enough to cause damage (perhaps in the form of PR, or obtaining information that can be used against the company, etc.)

While many of the perpetrators of such break-ins are merely thrill-seekers interested in nothing more than seeing the shell prompt of your computer on their screen, there are those who are more malicious, as we shall examine next. Additionally, keep in mind that it's possible that someone who is normally interested in nothing more than the thrill could be persuaded to do more: perhaps an unscrupulous competitor is willing to hire such a person to hurt you.

Destructive Behavior

Among the destructive sorts of break-ins and attacks, there are two major categories: Data Diddling and Data Destruction, which are discussed below.

DATA DIDDLING

The data diddler is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plans. May be he is changing the account numbers for the auto-deposit of certain pay cheques. In any case, rare is the case when you'll come in to work one day, and simply know that something is wrong. An accounting procedure might turn up a discrepancy in the books three or four months after the fact. Trying to track the problem down will certainly be difficult, and once that problem is discovered, how can any of your numbers from that time period be trusted? How far back do you have to go before you think that your data is safe?

DATA DESTRUCTION

Twisted jerks simply like to delete things. Some perpetrate attacks. In these cases, the impact on your computing capability – and consequently your business – can be nothing less than if a fire or other disaster caused your computing equipment to be completely destroyed.

Gaining Access

How does an attacker gain access to your computer? He can gain access through any connection that you have to the outside world. Internet connections, dial-up modems, and even physical access are included.

All possible avenues of entry must be identified and evaluated to adequately address security. The security of that entry point must be consistent with your stated policy on acceptable risk levels.

CAUSES OF RISKS

The risks are caused by:

a. **Virus attacks:** This has already been discussed at length in the previous section in this chapter.

b. **Intruders:** It is explained in the following paragraphs.

Intruders

One of the two most popular threats to a network's security is the intruder (the other being viruses), generally referred to as hacker or cracker. The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. There are three types of intruders:

- *Masquerader:* An individual who is not authorized to use the computer penetrates a system's access controls to exploit a legitimate user's account.
- *Misfeasor:* A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- *Clandestine User:* An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Intrusion Techniques

There are two types of intrusion techniques: (i) One-way encryption and (ii) Access control.

- *One-way encryption:* The system stores only an encrypted form of user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.
- *Access control:* Access to the password file is limited to one or a very few accounts.

INTRUSION DETECTION

Eventually, the best intrusion prevention system will also fail. A system's second line of defense is intrusion, and this has been the focus of much research in recent years because of several reasons:

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner the intrusion is detected, the less the amount of damage and more quick the recovery.
- An effective intrusion detection system can serve as a deterrent, as such it can prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

The usual method to detect intrusion is by an audit trail, which is a chronological record of events occurring in a system. This record is maintained for tracing irregularities and to detect the consequences of error. It also facilitates monitoring of the system. There are two types of audit trails.

– *Accounting audit trail* – it maintains a record of processes that update the data and information.

– *Operations audit trail* – it maintains a record of attempted or actual consumption of resources within a system.

Usual audit trail containing details of both successful and unsuccessful transactions with terminal number, user-id, transaction details, time stamp and authentication particulars are generated by the system. As a security measure the audit trail should be properly scrutinized and particular care should be taken to ensure that transaction numbers are in running sequence and no number is missing.

CONTROL MEASURES

Information systems hardware, software, networks and data need to be protected by built-in controls to ensure their security. Effective controls ensure accuracy, integrity and safety of information system resources and activities associated with it. They can minimize errors, fraud, and destruction, in the Internet worked information systems. Different types of contols are available in administrative and software security. They are:

- Input controls,
- Output controls,
- Procedural controls,
- Facility controls.

Input Controls

Input controls are usually set in the form of login passwords and other security codes, formatted data entry screens, error signals, etc. Processing controls are developed to identify errors in arithmetic calculation and logical operations. They also ensure that data is not lost, or that it does not go unprocessed. Process controls can be either hardware controls or software controls.

Output Controls

Output controls are developed to ensure that information products are correct and complete, and are available only to authorized users in a timely manner. Access to online output of computer networks is generally controlled by security codes that identify the type of output. 'Pre numbered output forms' is another method that can be employed to check the loss of important output documents. Typically, operating systems or security monitors protect the databases of real time processing systems from unauthorized use or processing accidents. Account codes, passwords and other security codes are frequently used to ensure that only authorized users are granted access.

Procedural Controls

These help to ensure the accuracy and integrity of computer and network operations and systems development activities. Use of standard procedures and documentation helps in promoting quality and minimizing chances of error or fraud. It enables both end users and IS specialists know what is expected of them.

Natural or man-made disasters may sometimes cause severe damage to an organization's computing resources. Many mission-critical applications in airlines, banks or defence services must be protected from being affected by such calamities. Organizations therefore, need to develop disaster recovery procedures and plans. These procedures and plans specify the employees who will participate in disaster recovery and their responsibilities, the hardware and software facilities to be used.

Facility Controls

Computer networks and other hardware are subject to hazards such as accidents, natural disasters, sabotage, industrial espionage, destruction or theft. Various safeguards and control procedures are necessary to protect the hardware, software, network and vital data resources of an organization. Thus a specialized system software packages known as system security monitors provide security for a network. These are programs that monitor the use of computer systems and networks and protect them from unauthorized use, fraud or destruction. Two most commonly used methods in network security are *encryption* and *firewalls*.

Every control measure falls into the above four categories but again each falls under one of the two categories – either system level or the network level;

SYSTEM LEVEL CONTROLS

System level security is concerned with the level of a standalone system/terminal. The normally used control measures at a system level are Passwords, Antiviruses, and Firewalls, etc.

Passwords

The front line of defense against intruders is the password system. The password serves to authenticate the ID of the individual and logging on to the system. In turn, the ID provides security in the following ways:

– The ID determines whether the user is authorized to gain access to a system. In some systems, only those who already have an ID filed on the system are allowed to gain access.

– The ID determines the privileges accorded to the user. A few users may have supervisory or 'super user' status that enables them to read files and perform functions that are especially protected by the operating system. Some systems have guest or anonymous accounts and the users of these accounts have more limited privileges than others.

– The ID is used in what is referred to as discretionary access control. For example, by listing the Ids of the users, a user may grant permissions to them to read files owned by that user.

Password Selection Strategies

Many users choose a password that is too short or too easy to guess. At the other extreme, if users are assigned passwords consisting of eight randomly selected printable characters, password cracking is effectively impossible. But it would be almost as impossible for most users to remember their passwords. Fortunately, even if we limit the password, the universe is still too large to permit practical cracking. Hence our goal is to eliminate guessable passwords while allowing the user to select a password that is memorable.

Antiviruses

The ideal solution to the threat of viruses is prevention – do not allow a virus to get into the system in the first place. This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks. The next best approach is to be able to do the following:

Detection: Once the infection has occurred, determine that it has occurred and locate the virus.

Identification: Once the detection has been made, identify the specific virus that has infected a program.

Removal: Once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state. Remove the virus from all infected systems so that it cannot spread further.

If detection succeeds but either identification or removal is not possible, then the alternative is to discard the infected program and reload a clean back-up version. Advances in virus and antivirus technology go hand in hand. Early viruses were relatively simple code fragments and could be identified and purged with relatively simple antivirus software packages. As the virus arms race has evolved, both viruses and, necessarily, antivirus software have grown more complex and sophisticated.

Two most popularly used advanced antivirus techniques used in the present-day are generic decryption and digital immune system.

Generic Decryption

This technology enables the antivirus program to detect easily the most complex polymorphic viruses while maintaining fast scanning speeds. When a file containing a polymorphic virus is executed, the virus must decrypt itself to activate. In order to detect such a structure, executable files are run through a GD scanner, which contains the following elements: CPU emulator, Virus signature scanner and Emulation control module.

Digital Immune System

The digital immune system is a comprehensive approach to virus protection developed by IBM. The motivation for this development has been the rising threat of Internet-based virus propagation. The objective of this system is to provide rapid response time so that viruses can be stamped out as soon as they are introduced. When a new virus enters an organization, the immune system automatically captures it analyzes it, adds detection and shielding for it, removes it, and passes information about that virus to systems running antivirus softwares so that it can be detected before it is allowed to run elsewhere.

NETWORK LEVEL CONTROLS

The other types of classification of security measures, apart from the system level, are the network level security measures. They provide security to network and the elements of a network as a whole. For this purpose either firewalls or cryptographic techniques are used.

Firewalls

A firewall is the point at which your private company network and a public network, such as the Internet, connect. A firewall system is a hardware/software configuration, which sits at this perimeter, controlling access into and out of your company's network. New ways are constantly being developed to compromise these systems while in theory, firewalls allow only authorized communications between the internal and external networks. However, properly implemented they are very effective at keeping out unauthorized users and stopping unwanted activities on an internal network. Firewall systems can also be deployed within an enterprise network to compartmentalize different servers and networks, in effect controlling access within the network. For example, an enterprise may want to separate the accounting and payroll server from the rest of the network and only allow certain individuals to access the information.

Firewall Systems Protect and Facilitate the Network at a Number of Levels

- They allow e-mail, and other applications such as FTP and remote login as desired, to take place while otherwise limiting access to the internal network.
- They provide an authorization mechanism, which provides a level of assurance that only specified users or applications, can gain access through the firewall.
- They typically provide a logging and alerting feature, which tracks designated usage and signals at specified events.

- They offer address translation, which masks the actual name and address of any machine communicating through the firewall. For example, all messages for anyone in the technical support department would have their address translated to techhelp@company.com, effectively hiding the name of an actual user and network address.
- They add new functionality, such as encryption and virtual private networks capabilities. Encryption is the coding, or scrambling, of data and keeps unintended users from reading the information. Virtual Private Networks employ encryption to provide secure transmissions over public networks such as the Internet.
- Finally, you should consider that all firewall systems have some performance degradation. As a system is busy checking or re-routing data communications packets, they do not flow through the system as efficiently as they would if the system were not in place.

Firewalls can be an effective means of protecting a local system or a network of systems from network-based security threats while at the same time affording access to the outside world.

CHARACTERISTICS

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
- The firewall itself is immune to penetration. This implies the use of a trusted system with a secure operating system.

THE CAPABILITIES OF FIREWALL CONFIGURATIONS

- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
- A firewall provides allocation for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
- A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

THE LIMITATIONS OF FIREWALLS

- The firewall cannot protect against the things that bypass it. Internet systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-up capability for traveling employees and telecommuters.
- The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

TYPES OF FIREWALLS

The three common types of firewalls are: (i) Packet-filters, (ii) Application-level gateways, and (iii) Circuit-level gateways.

- *Packet-filtering Routers:* A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on fields in IP and transport (for example, TCP or UDP) header, including source and destination IP address, IP protocol filed and TCP port number.

  The packet filter is typically set-up as a list of rules based on matches to fields in the IP or TCP header. If there is no match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

- *Application-level Gateway:* Also called a proxy server, it acts as a relay. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two end points.

  These application-level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level.

  A prime disadvantage of this type of gateway is the additional processing over-head on each connection. In effect, there are two spliced connections between the end-users, with the gateway at the slice point, and the gateway must examine and forward all traffic in both directions.

- *Circuit-level Gateway:* The third type of firewall is the circuit-level gateway. This can be a standalone system or a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

  A typical use of the circuit-level gateways is a situation in which the system administrator trusts the internal users.

FIREWALL CONFIGURATIONS

In addition to the use of a simple configuration consisting of a single system, such as a single packet-filtering router or a single gateway, more complex configurations are possible.

Screened Host Firewall (Single-homed) – This configuration affords flexibility in providing direct Internet access. The internal network may include a public information server, such as a web server, for which a high-level of security is not required. In that case, the router can be configured to allow direct traffic between the information server and the Internet.

Screened Host Firewall (Dual-homed) – In the above configuration if the packet-filter router is completely compromised, traffic could flow directly through the router between the Internet and other hosts on the private network. But this configuration prevents such a security breach.

Screened Subnet Firewall Configuration – This is the most secure configuration. Both the Internet and the internal network have access to hosts on the screened

subnet, but traffic across the screened subnet is blocked. This configuration has some advantages like – there are three levels to thwart intruders. The outside router advertises only the existence of the screened subnet to the Internet; therefore, the internal network is invisible to the Internet.

Cryptography

The process of systematic encoding of data before transmission so that an unauthorized person cannot decipher it is called as data encryption. There are different types of encryption techniques but each is suitable depending upon the situation.

In the process of sending a message, the sender sends the encrypted data that is governed by an algorithm and has a key, which is changed periodically. At the receiving end that data is decrypted using the key. Because the key is the only means that can decrypt the encoded message there is very little or no chance for the hackers to decrypt. And there is no compulsion that the sender and the receiver should be at standard spots.

Approaches that Use Conventional Encryption

It is possible to perform authentication simply by the use of conventional encryption. If we assume that only the sender and the receiver share a key (which is as it should be), then only the genuine sender would be able to encrypt a message successfully for the other participant. Furthermore, if the message includes an error-detection code and a sequence number, the receiver is assured that no alterations have been made and that sequencing is proper. If the message also includes a timestamp, the receiver is assured that the message has not been delayed beyond what is normally expected for network transit.

Encryption Techniques

The Internet is a public network and raw data transmitted over it is liable to be intercepted by unauthorized persons (called eavesdropping). Such eavesdropping can be avoided if by some means one is able to send the data in a ‘secret’ or ‘coded’ fashion over the Internet. Encryption techniques seek to do this thereby ensuring secure transmission of data (like the payment related data in payment gateways) on the Internet.

Encryption is the transformation of data into a form that is nearly impossible to decipher without the use of one or more keys (specialized data chunks). Decryption is the reverse of encryption; it is the transformation of encrypted data back into an intelligible form. The two most commonly used techniques of encryption are described as follows:

– *Secret key or Private Key or Symmetric Key Cryptography:* In this encryption technique, there is a single key, called the secret key or private key or symmetric key, which is used for both encryption and decryption of the data. Hence, the sender and the receiver both must posses the same secret key. Secret key cryptography is not useful in large networks like the Internet.

  For example, an Internet shopping mall would have to assign consumer a distinct key. Hence secret key cryptography is possible in small networks where the involved parties know each other previously and can trust each other with the secret keys. An offline application of this is in encryption of customer PINs by financial institutions. Each customer is known to the financial institution and is given a PIN for identification, which is encrypted using secret key cryptography during transactions. The cryptographic algorithm used in this case is called Data Encryption Standard (DES).

  In the online world, both the Secure Sockets Layer and Secure Electronic Transaction technologies combine secret key cryptography as well as public key cryptography.

– *Public key or Asymmetric key Cryptography:* In this encryption technique, there are two keys, one a private or secret and the other a public key. The two keys form a pair such that the message encrypted by one key can be decrypted by the other. Generally the user confidentially retains the private key with himself while the public key is displayed publicly.

  For example, an online shopping mall can generate a public-private key pair and publish the public key on its website. A consumer can use the public key to send encrypted messages to the online shopping mall which only the mall can decrypt since it alone possesses the private or secret key to decrypt it. Thus, the consumer can be assured that the data will travel securely over the Internet and that only the online shopping mall would be able to receive and decrypt it. Clearly, public key cryptography is useful for large public networks like the Internet. The most popular cryptography algorithm used in case of public key cryptography is the RSA algorithm (developed in 1977), named after its developers Ronald Rivest, Adi Shamir, and Len Adleman, then professors at the Massachusetts Institute of Technology. Public key cryptography uses more computer resources than the private key cryptography. However, with the technological improvements in computers this difference is narrowing down and these days the speeds of public key cryptography are quite acceptable. At the same time, use of public key cryptography on the Internet results in more secure messaging as compared to private key cryptography.

DISASTER RECOVERY, CONTINGENCY, AND EMERGENCY PLANS

The disaster recovery plan is a document containing procedures for emergency response, extended back-up operations, and recovery, should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. To provide for processing at an alternative site during the time that the original facility is unavailable is a key part of disaster recovery planning.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that defines the condition and response required to return a computing capability to nominal operation. An emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

SECURITY AND LEGAL FRAMEWORK

Connectivity via the Internet has greatly abridged geographical distances and made communication even more rapid. The law governing commercial transactions has to be consistent irrespective of the jurisdiction in which the trading partners reside. A security policy framework is necessary to support the security infrastructure required for the secure movement of sensitive information across and within national boundaries. To ensure the secure operation of this kind of infrastructure, it is necessary to have some well-founded practice for the identification of security risks (as well as the application of appropriate controls to manage risks).

This practice can be formalized and (semi-) automated by the use of formal methods and tools, which increase the reliability of the system specification (and therefore users' confidence in it). This is important since the security of a system is largely dependent upon the accuracy of its specification. To be truly beneficial, the

risk analysis framework must be granular enough to produce a customizable roadmap of the kind of problems that exist, and to rank them in order of severity, which facilitates making decisions about the ones that should be dealt with first. Its main objective is to develop a practical (the word practical emphasized) framework for a precise, unambiguous and efficient risk analysis, by exploiting the synthesis of risk analysis methods with object-oriented modeling, (semi-) formal methods and tools, in order to improve the security risk analysis and security policy implementation of security-critical systems.

Since the critical infrastructures of, for example, medical services, banking and finance, gas and electricity industries, transportation, water, and telecommunications are making use of the public Internet for communication, and not in the least for the exchange of business, administrative and research information, it must be our aim to make these critical infrastructures totally secure and unassailable.

What kind of legal provisions support Internet banking in our country? India, as on date, does not have a specific law on Internet banking. The Reserve Bank of India, being the apex banking regulatory body, has recently formulated guidelines for Internet banking to be implemented in a phased manner by banks all over the county. Earlier, the RBI had constituted a 'Working Group on Internet Banking', which focused largely on three areas, namely technology, security, and legal issues as also regulatory and supervisory issues. Under the new guidelines, the technology and security standards set by the RBI include:

- Designation of a network and database administrator with clearly defined roles.
- Banks are also required to have a security policy duly approved by the board of directors.
- It is further required that banks segregate the duty of the security officer/ group dealing exclusively with the IT division which actually implements the computer system. Information systems will be audited by information systems auditor.
- Banks are also directed to introduce logical access control techniques for which they may have user-IDs, passwords, smart cards or biometric techniques.
- In order to avoid any direct link with the Internet, banks should use a proxy server type of firewall at least. For sensitive systems, an inspection firewall has been recommended. These include real time security alert.
- In order to avoid intrusions into networks by-passing the proxy server, the guidelines recommend that systems supporting dial-up services through modem on the same LAN as application server should be isolated.
- Public Key Infrastructure is the most favoured technology. However, until it is put in place, banks may use at least a 128-bit SSL (Secured Socket Layer). All unnecessary services on application server should be disabled.
- It is also important to log all Internet accesses including messages received. Security violations (suspected or attempted) should be reported and follow-up action to be taken should be kept in mind while framing future policies.
- Banks are required to review their security infrastructure and policies regularly.
- The information security officer and the information system auditor should undertake period penetration tests, including attempts to guess passwords, search for backdoor traps and commonly known holes in software, etc. Banks may also employ outside experts or 'ethical hackers' for the same.
- The RBI guidelines use the term 'ethical hackers'. It is surprising that the RBI guidelines encourage banks to employ ethical hackers despite the fact that the IT Act, 2000 has declared hacking as a penal offence punishable with imprisonment of three years and fine up to Rs.2 lakh, and that the new cyber law does not make any distinction between ethical and unethical hacking.

- The RBI guidelines further stipulate that there should be a proper system for storage of back-up data which should be tested time and again to ensure recovery without loss of transactions.
- Disaster recovery sites should be constituted in order to ensure continuity of business. Systems should be upgraded by installing patches released by developers to remove bugs and loopholes.
- In the light of the prevailing legal position, banks are obligated to establish identity and make enquiries about the potential customer. Accounts should be opened only after proper introduction and physical verification of the identity of the potential customer.
- Also, banks should adopt only the asymmetric crypto system for digital authentication as provided under Section 3(2) IT Act, 2000.
- Banks are also required to maintain secrecy and confidentiality of customers' accounts under the present legal system. However, there is a possibility that banks may not be able to meet this requirement.
- Banks are, therefore, directed to institute adequate risk control measures to manage the same. They must also notify their customers the timeframe and circumstances in which any stop payment instructions could be accepted.
- Banks should also insure themselves against unauthorized transfer of funds from customers account through hacking, and denial of service due to technological failure.
- It is important to note that there has not been any determination so far of the rights and liabilities of customers availing Internet banking services.
- Under the head of Regulatory and Supervisory Issues, the RBI guidelines recommend that the existing regulatory framework for banks shall be extended to Internet banking also.
- It has been further advised that only banks with licenses supervised in India and with a physical presence in India shall be allowed Internet banking with residents of India.
- The products should be made available only to account holders and should not be offered in other jurisdictions. The service offered should only pertain to local currency products.
- The 'out-in' and 'in-out' scenarios whereby banks offer cross-border jurisdiction are generally not permitted and the same approach shall be applicable to Internet banking also.
- However, these exceptions shall not be applicable to customers permitted to maintain their accounts with overseas banks. Indian banks will be allowed to offer Internet banking services to overseas customers if they satisfy both host and home supervisors.
- The RBI guidelines have also issued various other instructions to be followed by the banks. For instance, banks must seek prior permission from the RBI before offering Internet banking services.
- The application for such permission should indicate a business plan, analysis of cost and benefit, operational arrangements, third party service providers, and systems and control procedures, which the bank proposes to adopt.
- Any breach/failure of security systems and procedures must be reported to the RBI. The RBI guidelines on "Risks and Controls in Computers and Telecommunications" will also be applicable to Internet banking.
- Banks should develop outsourcing guidelines to manage risks arising out of third party service providers. Only institutions that are members of cheque-clearing systems in the country will be permitted to participate in inter-bank payment gateways for Internet payment.

- All intra-bank payments, credit card transactions and payments arising from cross-border e-commerce transactions shall be excluded from inter-bank payment gateways.
- In order to access the gateway through the computer system, the bank should use a least line network. A PKI system should be followed once it is implemented.
- The rights and liabilities of the payee, the payee's bank, participating banks, the service provider and banks themselves should be clearly defined.
- Banks must disclose risks, responsibilities and liabilities of customers through a disclosure template. Hyperlinks from bank's websites should be allowed only to those portals with which they have payment arrangement.

The aforesaid guidelines also are applicable to all forms of electronic banking. With the implementation of the RBI's guidelines, Internet banking is likely to get the required boost in our country.

Box 2: Read This if You Bank Online

It's a daylight bank robbery without guns or getaway vans! It's happening in the virtual world, but the victim gets the living daylights shocked out in real world. And all it takes is a laptop, a modem and an evil-genius mind.

Computer security experts have warned of Internet virus that steal password and account information of users who bank online. The latest bug, targets Internet Explorer browser users and can be picked up from pop-ads, which secretly download and install programs that read keystrokes and relay them to the hackers.

The pop-ups originate from websites that run ads from certain online ad services. These online ad servers apparently have themselves hacked to spread the bug. The virus reportedly has a list of about 50 banks. Once it detects the user logging into one of the banks, it reads login passwords and intercepts the information before it gets encrypted.

The earlier virus was of a different origin and was picked up from websites that were infected. However, the goal of both programs remains the same — to steal bank account information. The two attacks highlight new risks to transmission of sensitive financial information on the Internet, experts said.

Users working on Internet Explorer browsers are the main targets of this virus because of the flaws in the software. However, Microsoft has said that it has been able to fix two of the three flaws, the third one still exists. Experts say that using pop-up killers (software that block pop-up ads) can help in stopping the bug from infecting one's computer. Another option is to use a non-Microsoft browser, such as Netscape, Mozilla or Opera.

Internet Explorer users are immune if they download and install a patch. Experts have also advised Internet Explorer users to set the security setting for their browser to "high" level. A report on a website owned by Consumers' Institute of New Zealand, Inc, said a man from Auckland had his bank account robbed through the Internet in April this year.

Withholding his name, the website said $20,000 was transferred from his BNZ business account to a Kiwibank account. The Kiwibank account holder, an innocent third-party, had been duped by fraudsters. He in turn sent the money to a bank in Estonia.

The transfer reportedly happened on a Friday night and was cleared and gone by midnight. The following Monday, a second transfer occurred but was detected and reversed. The man's laptop, which did have anti-virus software, was found to be infected by a Trojan Horse program. The program may have come in as an email attachment or via a dodgy pop-up on a website advertising plasma TVs, the site reported.

The program read the keystrokes, which were recorded and transmitted back to the fraudsters, giving them access to his online banking details.

Source: http://www.rediff.com/money/2002/nov/15rbi4.ntm

Information Technology bill was enacted in Parliament, which deals with some of the issues mentioned above. The Act provides legal framework so that the information is not denied legal effect, validity or enforceability solely on the ground that it is in electronic form. This is done by validating and authorizing the use of Electronic Data Interchange (EDI), Electronic Records, and Electronic Signatures. The Information Technology Act, 2000, should escort the new era of e-commerce and e-governance as it provides rules for validation and recognition of contracts formed through electronic means and also supports the admissibility of computer evidence in the courts of law. The Act will also facilitate electronic filing of documents with the Government agencies.

The Act treats the following as offences related to the field of Information Technology.

- Failure to comply with CCA under the provisions of the Act, rules and regulations made there under.
- Any misinterpretation or suppression of facts for the purpose of obtaining any license or Digital Signature Certificate.
- Breach of confidentiality and privacy, i.e., disclosure of any electronic record, book, register, information, document or other material accessed/obtained without the consent of the person concerned.
- Hacking, i.e., destroying, deleting or altering any information residing in a computer resource that is declared to be a protected system by Government of India, from time to time.
- Knowingly creating, publishing or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.

There were many amendments made to the Acts formulated earlier. However, there is an urgent need to amend certain laws so as to make them in consonance with the Internet and so that electronic fund transfers are legal.

SECURITY POLICY

Everything discussed above involves specific things you can do, tools and techniques to implement, to address a particular area or hole in security. Security policy is what ties all into a cohesive and effective security program.

A security policy is a formal specification of the rules by which people are given access to a computer and its resources.

Developing a Security Policy

The first rule of network security is easily stated: That which is not expressly permitted is prohibited. Simply, a security policy should start by denying all access to all network resources, and then expressly add back access on a specific basis. Implemented in this way, your security policy will not allow any inadvertent actions or procedures.

The goal in developing a policy on computer security is to define the organization's expectations of proper computer network use and to define procedures to prevent and respond to security incidents. In order to do this, aspects of the particular organization must be considered and agreed upon by the policy making group.

- The goals and direction of the organization should be considered. For example, a military base may have very different security concerns from those of a university. For that matter, departments within the organization will have different requirements, and these should be considered as well.
- The security policy developed must conform to existing policies, rules, regulations, and laws that the organization is subject to. Therefore, it will be necessary to identify these and take them into consideration while developing the policy.

- Unless the local network is completely isolated and stand-alone, it is necessary to consider security implications in a more global context. The policy should address the issues when local security problems develop as a result of a remote site as well as when problems occur on remote systems as a result of a local host or user.
- It is important to consider who will make the network security policy. Policy creation must be a joint effort by a representative group of decision makers, technical personnel, and day-to-day users from different levels within the organization. Decision makers must have the power to enforce the policy; technical personnel will advise on the ramifications of the policy, and day-to-day users will have a say in how "usable" the policy is. A security policy, which is unusable, unimplementable, or unenforceable, is useless.

Developing a security policy involves identifying the organizational assets, and the threats, evaluating the risk, evaluating and implementing the tools and technologies available to meet the risks, and developing a usage policy. In addition, an auditing procedure must be created which reviews network and server usage on a timely basis. A response should be in place before any violation or breakdown occurs. Finally, the policy should be communicated to everyone who uses the computer network, whether employee or contractor, and the policy should be reviewed on a regular basis.

Identifying the Organizational Assets

The first step in creating a security policy is creating a list of all the things (assets) that need to be protected. The list needs to be regularly updated, as most organizations add and subtract equipment all the time. Items to be considered include:

- **Hardware:** CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers and routers.
- **Software:** Source programs, object programs, utilities, diagnostic programs, operating systems and communication programs.
- **Data:** During execution, stored on-line, archived off-line, back-ups, audit logs, databases, in transit over communication media.
- **People:** Users, people needed to run systems.
- **Documentation:** Of programs, hardware, systems and local administrative procedures.
- **Supplies:** Paper, forms, ribbons and magnetic media.

Assessing the Risk

While there is a great deal of discussion about intruders on computer networks, most surveys show that the actual loss from people within the organization is significantly greater. Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all risks, and ranking them as per the level of severity. This process involves making cost-effective decisions on what you want to protect. Possible risks to your network include, apart from those already discussed above:

- Unauthorized access.
- Unavailable service, which can include some or all network services, corruption of data, or a slowdown due to a virus.
- Disclosure of sensitive information, especially that which gives someone else a particular advantage, or theft of information such as credit card information.

Once the list has been prepared, the risk should be weighed against the importance of the resource. This will allow the policy makers to determine how much effort should be put in protecting the resource.

Defining a Policy for Acceptable Use

The tools and applications discussed in the previous section will form the technical foundation of a security policy. But this is only part of the solution, and how users interact with the network is just as important. The creation of a policy for acceptable use should consider the following:

- Who is allowed to use the resources?
- What is the proper use of the resources?
- Who is authorized to grant access and approve usage?
- Who may have system administration privileges?
- What are the users' rights and responsibilities?
- What are the rights and responsibilities of the system administrator vs. those of the user?
- What do you do with sensitive information?

When defining the users' rights and responsibilities, you may want to cover several issues as:

- The guidelines regarding resource consumption, whether users are restricted, and if so, what the restrictions are.
- What constitutes abuse in terms of system performance?
- Whether users are permitted to share accounts or let others use their accounts.
- How "secret" users should keep their passwords?
- How often users should change their passwords and any other password restrictions or requirements?
- Whether you provide back-ups or expect the users to create their own.
- Disclosure of information that may be proprietary.
- Statement on Electronic Mail Privacy (Electronic Communications Privacy Act). Specifically, does the company consider electronic mail private to each employee, or the property of the organization?
- Your policy concerning mail or postings to mailing lists or discussion groups (obscenity, harassment, etc.), and on representing the organization to these areas.
- Policy on electronic communications: mail forging, etc.

It is important to define who will interpret the policy. This could be an individual or a committee. No matter how well-written, the policy will require interpretation from time to time and this body would serve to review, interpret, and revise the policy as needed.

Auditing and Review

To help determine if there is a violation of your security policy, take advantage of the tools that are included with your computer and network. Most operating systems store numerous bits of information in log files. Examination of these log files on a regular basis is often the first line of defense in detecting unauthorized use of the system.

Compare lists of currently logged-in users and past login histories. Most users typically login and out at roughly the same time each day. An account logged in outside the "normal" time for the account may be in use by an intruder.

Many systems maintain accounting records for billing purposes. These records can also be used to determine usage patterns for the system; unusual accounting records may indicate unauthorized use of the system.

System logging facilities, such as the UNIX "syslog" utility, should be checked for unusual error messages from system software. For example, a large number of failed login attempts in a short period of time may indicate someone trying to guess passwords.

Operating system commands which list currently executing processes can be used to detect users running programs they are not authorized to use, as well as to detect unauthorized programs which have been started by an intruder.

By running various monitoring commands at different times throughout the day, you make it hard for an intruder to predict your actions. While it may be exceptionally fortuitous that an administrator would catch a violator in the first act, by reviewing log files you have a very good chance to identify them at a later date.

Reviews are imperative due to today's changing computing environments. It is getting astoundingly easy to break into networks through available user-friendly point-and-click packages. Security is a dynamic process. Only by assembling the core team or a representative subset, and reviewing how well things are working, knowing about the latest threats and security tools, and assessing the risk against new assets and business practices, can an organization stay secure and productive.

Communicating to Users

The security policy should include a formalized process, which communicates the security policy to all users. In addition, an educational campaign should make users aware of how computer and network systems are expected to be used and how to protect themselves from unauthorized users.

All users should be informed about what is considered "proper" use of their account or workstation. This can most easily be done at the time a user receives his account, by sending him a policy statement. Proper use of policies typically dictate things such as whether or not the account or workstation may be used for personal activities (such as checkbook balancing or letter writing), whether profit-making activities are allowed, whether game playing is permitted, etc.

Users should be told how to detect unauthorized access to their account. If the system prints the last login time when a user logs in, he or she should be told to check that time and note whether or not it agrees with the last time he or she actually logged in. Ideally, the security policy should strike a balance between protection and productivity.

Violation Response

There are a number of responses, both good and sub-optimal, which an organization may choose upon realizing a site security violation. Planning responses for different scenarios well in advance – without the burden of an actual event – is a good practice. Not only do you need to define actions based on the type of violation, you also need to have a clearly defined series of actions based on the kind of user violating your computer security policy.

When a policy violation has been detected, the immediate course of action should be pre-defined to ensure prompt and proper enforcement. An investigation should be performed to determine how and why the violation occurred. Then, the appropriate corrective action should be executed. The type and severity of action taken varies depending on the type of violation that occurred.

Violation Discovery

Once a violation has been discovered, and is determined that it is being perpetrated by someone outside the organization, there are a number of aspects of your security plan that should be put in motion. Your security plan should be prepared to answer the following questions:

- Which outside agencies should be contacted, and who should contact them?
- Who may talk to the press?
- When do you contact law enforcement and investigative agencies?
- If a connection is made from a remote site, is the system manager authorized to contact that site?
- What are our responsibilities to our neighbors and other Internet sites?

Whenever a network suffers an incident, which may compromise computer security, the strategies for reacting may be influenced by two opposing pressures.

If the management fears that the network is sufficiently vulnerable, it may choose a *Protect and Proceed* strategy. This approach will have as its primary goal the protection and preservation of the facilities and to provide normalcy for its users as quickly as possible. Attempts will be made to actively interfere with the intruder's processes, prevent further access, and begin immediate damage assessment and recovery. This process may involve shutting down the facilities, closing off access to the network, or other drastic measures. The drawback is that unless the intruder is identified directly, he may come back via a different path or may attack another site.

The alternate approach, *Pursue and Prosecute*, adopts the opposite philosophy and goal. The primary goal is to allow intruders to continue their activities in the system until the responsible persons can be identified. Law enforcement agencies and prosecutors endorse this approach.

Prosecution is not the only outcome possible if the intruder is identified. If the culprit is an employee or a student, the organization may choose to take disciplinary action. The computer security policy needs to spell out the choices and how and which will be selected if an intruder is caught.

The management a strategy that must adopt might depend upon each circumstance. Or there may be a global policy, which mandates one approach in all circumstances. The pros and cons must be examined thoroughly and the users of the facilities must be made aware of the policy so that they understand their vulnerabilities no matter which approach is taken.

SUMMARY

- A gap in security can be defined as illegal access to information that can result in disclosure, obliteration, or alteration of that information. In other words, it occurs when information or systems are used or accessed for illegal purposes or for purposes they are not supposed to be used for. The common effects of the risks are – Violation of privacy, improper decision making leading to setback of business, financial loss due to computer frauds, interruption in activities due to loss of data, Hardware, Software and People ware.
- Some of the sources and types of network risks are denial of service, unauthorized access, executing of commands illicitly, confidentiality breaches and destructive behavior like data diddling and data destruction. And the main causes of risks are intruders and virus attacks.
- The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. The different types of intruders are masquerader, misfeasor and clandestine user. Effective controls ensure accuracy, integrity and safety of information system resources and activities associated with it. The different types of controls that are available in administrative and software security are: input controls, output controls, procedural controls and facility controls. The front line of defense against intruders is the password system. The password serves to authenticate the ID of the individual logging on to the system. ID determines the privileges accorded to the user. A few users may have supervisory or 'super user' status that enables them to read files and perform functions that are especially protected by the operating system. Some systems have guest or anonymous accounts and the users of these accounts have more limited privileges than others.
- The threat from viruses may take different forms: malicious programs, trap doors, logic bomb and Trojan horses. Viruses can be parasitic, memory-resident, boot sector, stealth and Polymorphic. They are classified according to their nature as: dormant phase, propagation phase, triggering phase and

execution phase. The ideal solution to the threat of viruses is prevention – do not allow a virus to get into the system in the first place. This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks. The next best approach is to be able to do the following – detection, identification and removal.

- Firewalls can be an effective means of protecting a local system or a network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. The different types of firewalls are packet-filtering routers, application level gateway and circuit level gateway.
- The process of systematic encoding of data before transmission so that an unauthorized person cannot decipher it is called as data encryption. There are different types of encryption techniques but each is suitable depending upon the situation. The two most commonly used types of techniques encryption are described as follows: Secret key or Private key or Symmetric key Cryptography and Public key or Asymmetric key Cryptography.
- The primary objective of a disaster recovery plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. There are several choices in disaster recovery plans and the choice is to be made depending upon the situation.
- A security policy framework is necessary to support the security infrastructure required for the secure movement of sensitive information across and within national boundaries. To ensure this it is necessary to have some well-founded practice for the identification of security risks (as well as the application of appropriate controls to manage risks). The three basic building blocks in the regulatory framework for e-commerce security are – (a) National cyber laws; (b) International treaties, understanding and collaborations in this regard; and (c) Administrative set-up for enforcement of the laws.
- The RBI has set-up new guidelines and security standards for the technology to be implemented in a phased manner all over. The guidelines are applicable to all forms of electronic banking as well. Further, the IT bill provides legal framework so that the information is not denied legal effect, validity or enforceability solely on the ground that it is in electronic form.
- The goal in developing a policy on computer security is to define the organization's expectations of proper computer and network use and to define procedures to prevent and respond to security incidents. Developing a security policy involves identifying the organizational assets, identifying the threats, evaluating the risk, evaluating and implementing the tools and technologies available to meet the risks, and developing a usage policy. An organization's assets include its hardware, software, people, data, documentation, etc. Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of your risks, and ranking those risks by level of severity.
- Once a violation has been discovered, and it is determined that it is being perpetrated by someone outside the organization, there are a number of aspects of your security plan that should be put in motion. The strategy adopted by the management might depend upon each circumstance. Or there may be a global policy, which mandates one approach in all circumstances. Reviews are imperative due to the ever-changing computing environments. It is getting astoundingly easy to break into networks through available user-friendly point-and-click packages.

Appendix I

Types of Risks Associated with Internet Banking

The rapid spread of I-banking all over the world is its acceptance as an extremely cost effective delivery channel of banking services as compared to other existing channels is a major driving force. However, Internet is not an unmixed blessing to the banking sector. Along with reduction in cost of transactions, it has also brought about a new orientation to risks and even new forms of risks to which banks conducting I-banking expose themselves. Regulators and supervisors all over the world are concerned that while banks should remain efficient and cost effective, they must be conscious of different types of risks this form of banking entails and have systems in place to manage the same. An important and distinctive feature is that technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures. Both evolve continuously. The thrust of regulatory action in risk control has been to identify risks in broad terms and to ensure that banks have minimum systems in place to address the same and that such systems are reviewed on a continuous basis in keeping with changes in technology. In the following paragraphs a generic set of risks are discussed as the basis for formulating general risk control guidelines, which this group will address.

Operational Risk: Operational risk, also referred to as transactional risk is the most common form of risk associated with I-banking. It takes the form of inaccurate processing of transactions, non-enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access/intrusion to bank's systems and transactions etc. Such risks can arise out of weaknesses in design, implementation and monitoring of banks' information system. Besides, inadequacies in technology, human factors like negligence by customers and employees, fraudulent activity of employees and crackers/hackers etc., can become potential sources of operational risk. Often there is a thin line of difference between operational risk and security risk and both terminologies are used interchangeably.

Security Risk: Internet is a public network of computers, which facilitates flow of data/ information and to which there is unrestricted access. Banks using this medium for financial transactions must, therefore, have proper technology and systems in place to build a secured environment for such transactions.

Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, etc. A breach of security could result in direct financial loss to the bank. For example, hackers operating via the Internet, could access, retrieve and use confidential customer information and can also implant virus. This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service, incurring costs to repair these etc. Other related risks are loss of reputation, infringing customers' privacy and its legal implications etc. Thus, access control is of paramount importance. Controlling access to banks' system has become more complex in the Internet environment which is a public domain and attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. Also, in a networked environment the security is limited to its weakest link. It is therefore, necessary that banks critically assess all interrelated systems and have access control measures in place in each of them.

In addition to external attacks, banks are exposed to security risk from internal sources, for example, employee fraud. Employees being familiar with different systems and their weaknesses become potential security threats in a loosely

controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank.

Unless specifically protected, all data/information transfer over the Internet can be monitored or read by unauthorized persons. There are programs such as 'sniffers', which can be set-up at web servers, or other critical locations to collect data like account numbers, passwords, account and credit card numbers. Data privacy and confidentiality issues are relevant even when data is not being transferred over the net. Data residing in web servers or even banks' internal systems are susceptible to corruption if not properly isolated through firewalls from Internet.

The risk of data alteration, intentionally or unintentionally, but unauthorized is real in a networked environment, both when data is being transmitted or stored. Proper access control and technological tools to ensure data integrity is of utmost importance to banks. Another important aspect is whether the systems are in place to quickly detect any such alteration and set the alert.

Identity of the person making a request for a service or a transaction as a customer is crucial to legal validity of a transaction and is a source of risk to a bank. A computer connected to Internet is identified by its IP (Internet Protocol) address. There are methods available to masquerade one computer as another, commonly known as 'IP Spoofing'. Likewise, user identity can be misrepresented. Hence, authentication control is an essential security step in any e-banking system.

Non-repudiation involves creating a proof of communication between two parties, say, the bank and its customer, which neither can deny later. Banks' system must be technologically equipped to handle these aspects, which are potential sources of risk.

System Architecture and Design: Appropriate system architecture and control is an important factor in managing various kinds of operational and security risks. Banks face the risk of wrong choice of technology, improper system design and inadequate control processes. For example, if access to a system is based on only an IP address, any user can gain access by masquerading as a legitimate user by spoofing IP address of a genuine user. Numerous protocols are used for communication across Internet. Each protocol is designed for specific types of data transfer. A system allowing communication with all protocols, say, HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), Telnet etc., is more prone to attack than one designed to permit, say, only HTTP.

Choice of appropriate technology is a potential risk banks face. Technology which is outdated, not scalable or not proven could land the bank in investment loss, a vulnerable system and inefficient service with attendant operational and security risks and also risk of loss of business.

Many banks rely on outside service providers to implement, operate and maintain their e-banking systems. Although this may be necessary when banks do not have the requisite expertise, it adds to the operational risk. The service provider gains access to all critical business information and technical systems of the bank, thus making the system vulnerable. In such a scenario, the choice of vendor, the contractual arrangement for providing the service etc., become critical components of banks' security. Bank should educate its own staff and avoid over-dependency on these vendors should be avoided as far as possible.

Not updating the bank's system in keeping with the rapidly changing technology, increases operational risk because it leaves holes in the security system of the bank. Also, staff may fail to understand fully the nature of new technology employed. Further, if updating is left entirely at customers' end, it may not be updated as required by the bank. Thus educating the staff as also the users plays an important role to avoid operational risk.

Approaches to reduce security related operational risk have already been discussed in detail in this Chapter. These include access control, use of firewalls, cryptographic techniques, public key encryption, digital signature etc.

Reputational Risk: Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions wherein public loses confidence in the banks' ability to perform critical functions or impair bank-customer relationship. It may be due to banks' own action or due to third party action.

The main reasons for this risk may be because the system or the product is not working to the expectations of the customers, due to significant system deficiencies, significant security breach (both due to internal and external attack), inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no alternative means of account access. Such situation may result in the customer discontinuing use of product or the service. Directly affected customers may leave the bank and others may follow if the problem is publicized.

Other reasons include losses to similar institutions offering similar type of services causing customer to view other banks also with suspicion, targeted attacks on a bank like hacker spreading inaccurate information about bank products, a virus disturbing bank's system causing the system and data integrity problems etc.

Possible measures to avoid this risk are to test the system before implementation, back-up facilities, contingency plans including plans to address customer problems during system disruptions, deploying virus checking, deployment of ethical hackers for plugging the loopholes and other security measures.

It is significant not only for a single bank but also for the system as a whole. Under extreme circumstances, such a situation might lead to systemic disruptions in the banking system as a whole. Thus, the role of the regulator becomes even more important as not even a single bank can be allowed to fail.

Legal Risk: Legal risk arises from violation of, or non-conformance of the laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established.

Given the relatively new nature of Internet banking, rights and obligations in some cases are uncertain and applicability of laws and rules is uncertain or ambiguous, thus causing legal risk.

Other reasons for legal risks are uncertainty about the validity of some agreements formed via electronic media and law regarding customer disclosures and privacy protection. A customer, inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions.

In the enthusiasm of enhancing customer service, a bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer.

If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risks. A digital certificate is intended to ensure that a given signature is, in fact, generated by a given signer. Because of this, the certifying bank may become liable for the financial losses incurred by the party relying on the digital certificate.

Money Laundering Risk: As Internet banking transactions are conducted remotely, banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus, banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with "know your customer" laws.

To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

Cross-Border Risks: Internet banking is based on technology that, by its very nature, is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders. This causes various risks.

It includes legal and regulatory risks, as there may be uncertainty about legal requirements in some countries and jurisdiction ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risks associated with non-compliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.

If a bank uses a service provider located in another country, it will be more difficult to monitor it thus, causing operational risk. Also, the foreign-based service provider or foreign participants in Internet banking are sources of country risk to the extent that foreign parties become unable to fulfill their obligations due to economic, social or political factors.

Cross-border transaction accentuates credit risk, since it is difficult to appraise an application for a loan from a customer in another country compared to a customer from a familiar customer base. Banks accepting foreign currencies in payment for electronic money may be subjected to market risk because of volatilities in foreign exchange rates.

Strategic Risk: This risk is associated with the introduction of a new product or service, and its degree of risk depends upon how well the institution has addressed the various issues related to development of a business plan, availability of sufficient resources to support this plan, credibility of the vendor (if outsourced) and level of the technology used in comparison to the available technology etc.

For reducing such risk, banks need to conduct proper survey, consult experts from various fields, establish achievable goals and monitor performance. Also they need to analyze the availability and cost of additional resources, provision of adequate supporting staff, proper training of staff and adequate insurance coverage. Due diligence should be observed in selection of vendors, audit of their performance and establishing alternative arrangements for possible inability of a vendor to fulfill its obligation. Besides this, periodic evaluations of new technologies and appropriate consideration for the costs of technological upgradation are required.

Other Risks: Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in Internet banking. These risks get intensified due to the very nature of Internet banking on account of use of electronic channels as well as absence of geographical limits. However, their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational and legal risks. This may be particularly true for banks that engage in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in Internet banking.

Credit risk is the risk that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks may not be able to properly evaluate the creditworthiness of the customer while extending credit through remote banking procedures, which could enhance the credit risk. Presently, banks generally deal with more familiar customer base. If a third party intermediary fails to carryout its obligations with respect to payment, facility of electronic bill payment in Internet banking may cause credit risk. Proper evaluation of the creditworthiness of a customer and audit of lending process are a must to avoid such risk.

Electronic money is another facility of Internet banking. It brings various types of risks associated with it. If a bank purchases e-money from an issuer in order to resell it to a customer, it exposes itself to credit risk in the event of the issuer defaulting on its obligation to redeem electronic money.

Liquidity risk arises out of a bank's inability to meet its obligations when they become due without incurring unacceptable losses, even though the bank may ultimately be able to meet its obligations. It is important for a bank engaged in electronic money transfer activities to ensure that funds are adequate to cover redemption and settlement demands at any particular time. Failure to do so, besides exposing the bank to liquidity risk, may even give rise to legal action and reputational risk.

Similarly, because of adverse movements in interest rates causing decrease in the value of assets relative to outstanding electronic money liabilities, banks dealing in electronic money face *interest rate risk*. Banks also face *market risk* because of losses in on-and-off balance sheet positions arising out of movements in market prices including foreign exchange rates. Banks accepting foreign currency in payment for electronic money are subject to this type of risk.

Risk of Unfair Competition: The competition among various banks is going to be intensified by Internet banking. Few banks may use unfair practices to take advantage over rivals as Internet is of open nature. Any leaks at network connection or operating system etc., may allow them to interfere in a rival bank's system.

Thus one can find that along with the benefits, Internet banking carries various risks for the bank itself as well as banking system as a whole. The nature and scope of risks banks face is likely to keep changing the rapid pace of technological innovation. These risks must be balanced against the benefits. Supervisory and regulatory authorities are required to develop methods for identifying new risks, assessing risks, managing risks and controlling risk exposure. But authorities need to consider the fact that the development and use of Internet banking are still in their early stages, and policies that hamper useful innovation and experimentation should be avoided. Thus, authorities need to encourage banks to develop a risk management process that is rigorous and comprehensive enough to deal with known risks and flexible enough to accommodate changes in the type and intensity of the risks.

Chapter V

Recent Trends of IT in Banking

After reading this chapter, you will be conversant with:

- The Branch Renaissance
- The Migration to an Online Environment
- Customer Relationship through Portals
- The Digital Age of Banking

With advances in telecommunications systems and digital technology, it is difficult to predict how electronic banking will improve and expand in the future. For example, Internet banking via mobile phones using Wireless Application Protocol (WAP) or banking services through the TV screen via the new interactive TV channels may become established. It is expected that the number of customers who wish to bank online will increase, which could necessitate personalized services and better online customer care from traditional high street banks. To combat computer crime and increasing security concerns, banks may consider new security measures such as iris, voice and fingerprint recognition, smart cards and electronic signatures.

In the last couple of decades, IT has become an integral part of a financial institution's competitive advantage. During the 1990s, efficiency and cost-cutting used to be the primary objectives of IT. Owing to relatively strong performance during the economic downturn, banks have been able to evolve a strategic approach towards their investments in IT. In their quest for better ROI, the revenue enhancement and cost-cutting are given equal weight when considering investment projects.

THE BRANCH RENAISSANCE CONTINUES

In the presence of e-banking banks also are recognizing that the branch is still the cornerstone of retail banking. Banks are focusing their efforts on improving revenues through sales of complex higher-margin services and products, and they are finding that branch is the most effective delivery channel for this purpose. The direct personal interaction provided at the branch provides the best environment for selling such products. Their ability to leverage the branch, however, has been impeded by legacy systems and outdated applications as they no longer can support innovative delivery strategies. Therefore, banks, in order to successfully harness the branch's sales potential, will increasingly implement upgrades in branch technology.

Multi-channel integration has caught the attention of a growing number of banks. Although it is far from becoming a mainstream exercise, it is moving away from the early-adopter phase to being a feasible initiative for most banks to undertake. Second-wave adopters are moving gradually, due to the complexity and cost of integration. Many of these banks are moving ahead by relying on third-party solution providers. Internet banking and call center platforms are currently ripe targets for integration.

Saddled with the high costs and integration challenges associated with the antiquated core banking systems, banks are beginning to consider replacing these vital systems. A core system replacement can be a risky as well as costly IT project a bank can take on, hence many banks are moving in this direction cautiously. It is expected that over the next few years, an increasing number of banks around the globe will begin to take on such projects. They will consider for the first time a third-party solution, as opposed to building new proprietary solutions, which are believed to be too costly and risky. When the world's largest banks successfully complete their projects, setting an example for the industry, other smaller banks are likely to follow.

In the coming days most of the top banks will have a senior executive appointed to be the head of a payments council. He will play an increasing role in shaping a banks' strategies in the changing payment environment. The vast majority will not be able, however, to supersede business lines, and will still lack P&L responsibility. Probably, very large banks will be strengthening or building up a distinct payment business line across retail and wholesale payments.

Improvements in Internet Banking

Banks are increasingly convinced that ROI from Internet banking can extend beyond simple cost-to-serve equations and direct revenue models. Due to the enhancements in Internet banking and user-friendliness, Internet banking's ROI now is poised to generate revenues indirectly by improving customer satisfaction with Internet banking. This in turn will translate into greater customer retention and higher balances. Banks' expectations include lowering cost-to-serve through self-service features with broad appeal, and customer support features that not only improve customer service representatives' effectiveness but also their efficiency.

Expanding Automation of the Loan Process

As interest rates look up, banks are scrambling to develop marketing and IT strategies geared towards maintaining strong growth in originations. Next-generation solutions will provide users with greater work process automation capabilities and better integration with third party applications, thereby eliminating many of the manual processes still in place today. A large portion of the typical loan process is still conducted via phones and faxes, creating bottlenecks and unhappy customers, who expect greater speed. The new solutions can also be better integrated with the front end, facilitating greater straight-through processing.

Better Services to Small Businesses

So far, small businesses have been chronically underserved by banks. The classic example is the application of a retail Internet banking solution to serve these businesses, which has been the leading cause of low adoption to date. Banks, however, are increasingly recognizing they could garner a larger share of small businesses' financial services spending if they implement appropriate technology. In an effort to better serve them and attract their business, banks will deploy Internet banking solutions built specifically for small businesses. Thus, small business online banking adoption is expected to grow.

Check Imaging

With the help of latest technology, the full potential of check imaging technology can be realized. Check imaging, which had an ignominious start in the 1990s, is about to make a comeback driven by economic and technological factors. It began generating ripples in the late 1990s, with re-pass image capture and is currently propelling a tidal wave, which will sweep in check truncation and image exchange.

Cash Management

While most banks already have large corporate banking solutions in place, a large number of transactions are still being completed on Windows-based solutions. However, many banks are to migrate all of their customers over to browser-based solutions, because full functionality is available through this channel. As a result of this move the number of transactions online is expected to grow steadily. Cash management solutions are evolving, with the greatest advancements being made in FX capabilities, loan originations, and trade finance.

Convergence in Banking

By the turn of this twenty first century, the biggest banks in the industrial world have become complex financial organizations that offer a wide variety of services to international markets and control billions of dollars in cash and assets. Supported by the latest technology, banks are trying to identify new business niches, develop customized services, implement innovative strategies and exploit new market opportunities. With further globalization, consolidation, deregulation and diversification of the financial industry, the banking sector is likely to become more complex. Although, the banking industry does not operate in the same

manner all over the world, most bankers think about their corporate clients in terms of the following:

Commercial Banking: Commercial banking covers services such as cash management (money transfers, payroll services, bank reconcilement), credit services (asset-based financing, lines of credits, commercial loans or commercial real estate loans), deposit services (checking or savings account services) and foreign exchange.

Investment Banking: Investment banking covers an array of services ranging from asset securitization, coverage of mergers, acquisitions and corporate restructuring to securities underwriting, equity private placements and placements of debt securities with institutional investors.

Over the past decade or so there has been an increasing convergence between the activities of investment and commercial banks as a result of deregulation in the financial sector. These days we can find investment and commercial banking institutions compete directly in money market operations, private placements, project finance, bonds underwriting and financial advisory work.

The modern banking industry has brought greater business diversification. Some banks in the developed countries are entering into investments, underwriting of securities, portfolio management and the insurance businesses. These changes have made banks an even more important entity in the global business community.

THE MIGRATION TO AN ONLINE ENVIRONMENT

With the rapid shift of business into the online environment, the pressure to enhance market value, latest expansions and consolidations there can be no doubt that the current trends in retail banking are going to confront financial services providers. The important trend of customers increasingly prefering securities as investment vehicles, has been visible for the last ten years, but is now being significantly accentuated. Individually, each of these trends has already had or will have a considerable effect on retail business; combined together, they will ensure that banking landscape will experience greater change over the next five to ten years than experienced over the previous twenty years.

The latest innovations in technology, such as broadband transmission, WebTV and wireless Internet access via mobile phones (GSM or Fixed Wireless), will all provide further impetus to the digital revolution. Private customer business will also be very strongly influenced with the trends in Internet usage. As a result of these changes, the retail bank of the future will have little in common with the bank we know today, despite the fact that the bank of the future will still consist of "bricks" as well as "clicks". It is expected that in future the customer contact will increasingly be online, the Internet portal will be the preferred point of access to the bank, and providers will be quick to expand their product range to include both competitors' products and new, tailored value-added products.

New Distribution Channels

As mentioned above, Internet will become an essential access channel. The indirect influence of the Internet is going to be more powerful than its direct impact. It is expected that about 30–50% of banking business will be significantly effected through the Internet, as customers will gather information about particular products or services, compare several players in terms of price or performance, or visit virtual marketplaces that bring together supply and demand in various areas.

As more households will have broadband Internet connections, new approaches will evolve to provide advisory services. Data, voice and image will integrate and put the bank's branch on screen in the customer's living room. Customers will be able to see their advisor via image phone while, at the same time, the advisor will be able to send information to the customer over the Internet.

Banks will be able to serve their customers wherever they are. Customers' mobile phones will become their "pocket banks". The user-friendly larger screen phones are going to have permanent Internet access; thus, the next generation of mobile phones will give bank customers unrestricted access to the events and developments that they are interested in.

It is obvious that these developments will have a radical effect on the mix of distribution channels used by customers.

The outlook for branch networks is one of accelerated contraction. The pressure to reduce the branch network is accentuated by margin erosion, which is to be expected as a result of lower online prices, particularly in brokerage and finance. On average, margins in pure online channels are expected to fall by 20–40%, while the stationary and multi-channel margins can be expected to fall by 10%.

CUSTOMER RELATIONSHIP THROUGH PORTALS

A bank's Internet portal will become the cornerstone of the customer relationship, especially for a large part of the high-revenue customers. Customers can use the bank's portal for transactions as well as for information. They will also be able to configure the portals to suit their own requirements. Thus, they will have up-to-date information constantly available. The banks will be able to use the central data management tool to make personalized information available to their customers on their own "personal" portals, which means that the customers will have access to a wide range of improved options for managing their finances, as well as personally tailored product offers.

The more data a bank has on a customer, the better it can interpret it, and support the customer in personalizing his or her portal. The banks that can offer these services will enjoy a sustained competitive advantage.

Traditionally many banks have offered their own products. But, the retail bank of the future will offer its customers a selection of the best available products in any product category. The reasons are:

The new information media will make the product offer considerably more transparent. Already today, independent financial services providers offer their customers continuous comparisons of the products of various banks, at no charge. With the spread of the Internet, more and more customers will have access to this information, and be able to compare the products of different providers in "marketplaces" and make their purchases accordingly. If the banks do not want to endanger their customer relationships, they will have themselves to offer a broad range of the best financial products.

Owing to the cost and revenue pressure many banks can no longer be competitive with their own product portfolios. They will have to cooperate with other producers in order to have the necessary expertise and achieve economies of scale. Thus, product manufacture and distribution will increasingly be decoupled.

Alliances between financial service providers will generate a variety of value-added services and products, often on favorable terms. In the area of property intermediation and financing, for example, providers may offer virtual tours of the property, information on the surrounding area, or intermediation of removal services.

DIGITAL AGE

Welcome to the digital age of banking, which facilitates a faster and more efficient way to store, manage and view checks. Now the customers need not sift through a shoebox to review their canceled checks.

Banks believe that financial institutions will embrace digital checks quickly because image exchange – the exchange of images rather than original paper – is expected to cut the volume of paper in circulation, which will eventually reduce the costs related to transportation and check-processing.

Billion of checks are written annually and several people may physically handle a single check through its life cycle. On average, banks store three copies of each check written, thus, resulting in huge costs. In addition, banks are required by law to keep detailed paper records of bank statements, including copies of original checks. But now the laws are changing and the banks can use digital documentation instead of the paper ones.

Check imaging has taken off because of the huge customer-service lift it provides. As an added bonus, removing the paper from the check payment process enables banks to significantly reduce operational costs, creating a win-win situation for customers and banks.

Check Imaging

Banks are looking forward to the day when a scanned image of a check can be zapped to another bank, into the depository and then back to the customer's bank. To begin with, many banks already are allowing employees and customers to view digital images of checks online. As the number of online banking customers increases, so will the rate of replacement of original paper checks in monthly statements. The next step in the process will be the proliferation of scanned imaging, which works by scanning a check's front and back, then making it available at Web-based ATMs or bank-teller stations, a copy of which can be printed for customers upon request.

There are two technologies behind digital archiving, imaging and exchange: content management and Web services. Content management is actually a set of technologies for creating, managing, integrating, Web-enabling and delivering digital content to employees, customers and, in this case, check writers. The technology allows users to access, retrieve and move all kinds of digital images. On the other hand, a Web service is a technology that allows disparate computers to communicate easily or simply.

Content management and Web services, together, are making the digital evolution of banking real and immediate. However, the target of moving toward total digital banking is yet to be achieved, even though the cost savings and increased efficiencies are quite evident. Digital archiving and digital technologies will reduce labor and mailing costs and will help provide improved services to banking customers.

Mobile Banking

Consumers are becoming more tech-literate, buying mobile phones, toying with online trading and just as much in need of banking services as consumers anywhere. So banks are trying to harness banking and mobile telephony into a set of applications and services, called m-banking, and are expecting that the money will roll in.

That is what cell-phone operators and financial institutions have expected. However, the substance of their offering was quite different from what they promised. Though there were many plans to enhance mobile-banking offerings and services, in reality the initiatives were very restricted. As of now most applications were informative, such as bank balances or credit-card or bank accounts, rather than interactive services like buying or trading.

Experience about m-banking in European countries has not been positive. Egg, the British leader in on-line banking, decided to abort its mobile offering; like many other banks, it saw little enthusiasm for mobile banking among its customers.

Problems included technical issues, security concerns and cost constraints. WAP (Wireless Application Protocol) proved to be too slow and cumbersome to satisfy the customer on the go, and the displays on phone screens were user-unfriendly. In addition, security was an important consideration for people seeking to access personal financial data, and their concerns were not adequately addressed by purveyors of m-banking.

Costs exceed benefits

The most significant problem of m-banking was that costs exceeded perceived benefits. The charges for data transmittal are still too high to spur mobile banking in several countries. Only promotional offerings agreed between banks and companies can help enhance this business area.

From the banking industry's perspective, mobile banking is a significant investment for typically low levels of Return On Investment (ROI) because there are few banking services that a banking client might consider worth the extra fees involved. Yet, the other factors driving a renewed interest in m-banking are the quest for competitive advantage and the advent of new mobile technologies and standards. These include i-Mode (a protocol developed in Japan, graphically more attractive and easier to use than WAP), UMTS (Universal Mobile Telecommunications Service, the 3G evolution of GSM) and MMS (Multimedia Messaging System, an evolution of the wildly successful short messaging service, or SMS, originally targeted at young people).

Some Examples

Rabobank, one of the largest retail virtual banks in the Netherlands, has based its m-banking initiative on GPRS (General Packet Radio Services), a faster technology than WAP. To justify the investment, the bank has made a detailed study of what would appeal to its customers, then decided not to limit itself to "pure" banking services but to offer five different services: mobile-banking services, telecommunications service, sporting news via SMS alerts, premium SMS services for television game shows, and mobile access to e-mail and calendar information for Rabobank employees.

Italy's Banca Intesa launched a new mobile-banking service, Intesa Online Mobile, in December 2003. Its offerings include SMS, MMS, WAP and PDA (Personal Digital Assistant), but the MMS solution immediately takes center stage because Banca Intesa's offering is the first of its kind on mobile-banking platform that exploits MMS technology. Users will be able to visualize their financial and investment situation across a series of banking accounts and credit cards. The integrated investment statement includes currency, liquidity, mutual funds, equities and selected charts about portfolio evolution.

Until UMTS can resolve the problems of high cost and security uncertainty MMS solutions are the most attractive platform for mobile banking at least in the next two years.

SUMMARY

- With advances in telecommunication systems and digital technology, it is difficult to predict how electronic banking will improve and expand in coming years. It is likely that the number of business customers who would want to bank online will increase which could lead to high street banks offering personalized services and better online customer care. To combat computer crime and to increase security levels, banks may consider new security measures such as iris, voice and fingerprint recognition, smart cards and electronic signatures.
- Banks are increasingly convinced that ROI from Internet banking can extend beyond simple cost-to-serve equations and direct revenue models. Due to the enhancements in Internet banking and user-friendliness, Internet banking's ROI now is poised to generate revenues indirectly by improving customer satisfaction with Internet banking. This in turn will translate into greater customer retention and higher balances.
- With the help of latest technology, the full potential of check imaging technology can be realized. Check imaging, which had an ignominious start in the 1990s, is about to make a comeback driven by economic and technological factors. It began generating ripples in the late 1990s with re-pass image capture and is currently propelling a tidal wave, which will sweep in check truncation and image exchange.

- With further globalization, consolidation, deregulation and diversification of the financial industry, the banking sector is likely to become more complex. Although, the banking industry does not operate in the same manner all over the world, most bankers think about their corporate clients in terms of Commercial banking and Investment banking.
- With the rapid shift of business into the online environment, the pressure to enhance market value, latest expansions and consolidations there can be no doubt that the current trends in retail banking are going to confront financial services providers. The latest innovations in technology, such as broadband transmission, WebTV and wireless Internet access via mobile phones (GSM or Fixed Wireless), will all provide further impetus to the digital revolution. Internet will become an essential access channel. Banks will be able to serve their customers wherever they are.
- Traditionally many banks have offered their own products. But, the retail bank of the future will offer its customers a selection of the best available products in any product category. Owing to the cost and revenue pressure many banks can no longer be competitive with their own product portfolios. Alliances between financial service providers will generate a variety of value-added services and products, often on favorable terms.
- Banks believe that financial institutions will embrace digital checks quickly because image exchange, the exchange of images rather than original paper, is expected to cut the volume of paper in circulation, which will eventually reduce the costs related to transportation and check-processing. There are two technologies behind digital archiving, imaging and exchange: Content management and Web services. Content management is actually a set of technologies for creating, managing, integrating, Web-enabling and delivering digital content to employees, customers and, in this case, check writers. The technology allows users to access, retrieve and move all kinds of digital images. On the other hand, a Web service is a technology that allows disparate computers to communicate easily or simply.

Chapter VI

Facilities Management

After reading this chapter, you will be conversant with:

- Cost Reduction Exercise
- Role of Technology
- Significance of Computerization in Banks
- Finance Portals for the Banking Industry
- Multi-channel Operations (Remote Banking)
- The Regulatory Framework

This chapter focuses on the need to provide best services to the customer, at the least cost. Undoubtedly, this is made possible to the greatest extent by the technological advancements that have taken place. In this regard, we describe the various uses of technology-based services that help provide customer conveniences at relatively low costs. We also study the regulatory role played by the Reserve Bank of India for this purpose.

COST REDUCTION EXERCISE

Cost Reduction Exercises in banks comprise the following activities:

- Minimum flow (by proper layout design),
- Automation,
- Facilities optimization,
- Procedural formalities improvement for time delays,
- Levels of dealing in an ultimate transaction,
- Speed and accuracy of information (managed by a good database and well trained personnel), and
- Well coordinated functioning.

Disciplines like timeliness in operations, availability of personnel at required time, consistency in quality and appropriateness of activities reduce time and cost elements. Automation and Networking are long-term gains of cost effectiveness in addition to value generation.

In the traditional banking system, bank operated lock boxes were used by companies to collect their payments and ensure that the money was deposited quickly. In today's competitive marketplace, effective management of cash flow can make the difference between success and failure. Corporate billing departments would wait for the bank to overnight copies of their customers' bills, and then credit the customers' accounts. With new innovations in technology such as light rays, digital imaging, and voice recognition, companies can update their accounts several times a day, view images of the invoices, and even check the envelopes they arrived in, without the use of paper. As a result, they are substantially shrinking the time it used to take to credit accounts and make deposits. In short, they are getting their money more quickly, freeing up cash flow for other things.

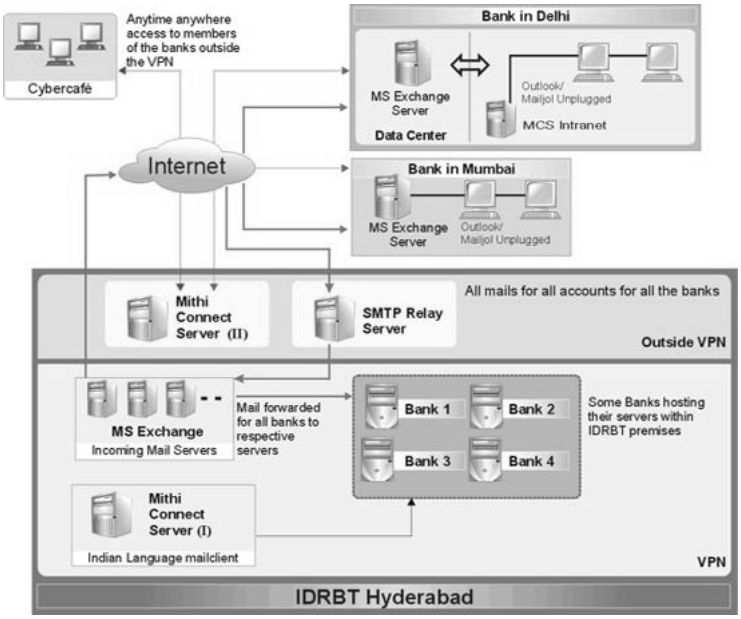
Some of the issues identified in the current set-up are cost of licensing more users on the MS Exchange server and availability of multilingual web mail access to their mailboxes. Some of the advantages would be:

i. Mail server would like to extend the number of users without having to pay heavy licensing fees while reliability and uptime are of prime importance.

ii. Banks would like to provide multilingual web mail client access to the mailboxes on the exchange servers for all users for anytime anywhere access. The web mail solution should be complete with support for folders, shared folders, search through messages, support for all Indian languages, etc. The web mail client should be customizable for each domain with the respective logos and color themes.

iii. It also helps in better management by way of obtaining usage reports, and is able to see live monitors of the server activity.

Figure 1: Mithi Connects Servers



Source:http://www.outlookmoney.com/scripts/IIH021C1.asp?sectionid=10&categoryid=124&articleid=5180

Acceptance

- Users on the Exchange Server Domains can log into the Mithi Web Mail via the respective Mithi Connect Server to view and work with their mailbox remotely.
- Users on Mithi Connect Server™ domains can login via the Mithi Web Mail to send and receive mail.
- Mail meant for the domains on Mithi Connect Server is received properly.

Benefits

- More users at a fraction of the cost of updating the licenses of MS Exchange, with similar ease of configuration and management via a web based console.
- Multilingual web mail to help them with access to mailboxes.
- Built in virus and spam control engines.
- Mithi Connect Server comes bundled with a firewall with a default high security configuration.

So, when a bank(er) plans a delight plan for its (his) customer, the focus would be on what attributes of service does he value, factors of importance to the customer (which varies in each of the category and the profile of the customer) and the relationship with the respective customer till date (if any). Banking still and in future, is nothing but people management, with banking as an apparent offering. The plan varies from customer to customer, based on his profile, to the service providers' (bankers') profile, objective/mission of the corporate body, relationship till date and macro environment conditions like fiscal rates, economic status, market trends, brand value of the bank, facilities offered and cost parameters and many other forces (situational/cultural/social etc.)

Some of the banks that provide best services to the customers are as follows:

- India's most customer-friendly bank is ICICI Bank, which outperforms even multinational banks.
- Ranking a close second is Citibank, which also tops the ranking of MNC banks on the overall score.

- For an entity that is not highly visible, seventh-ranked UTI Bank fares surprisingly well, breaking into the top 10 in all the six parameters on which the banks were rated.
- Strikingly, but not surprisingly, no nationalized bank figures in the top 10 banks, ranked on the overall score; the most customer-friendly PSU bank, Bank of Baroda, kicks in at No. 12; even the two banks (ING Vysya Bank and The South Indian Bank) that rank a joint 6th in the smaller universe of private banks score more overall than the top-ranked PSU bank.
- State Bank of India, by far India's largest bank, comes in a lowly 16th in the overall rankings; even among the smaller universe of PSU banks, it ranks only 5th, despite the fact that the survey methodology assigned some weightage to the size to acknowledge big banks' problems in servicing a large customer base.
- It is not as if the entire universe of PSU banks is uniformly insensitive to customers' expectations on service quality. Bank of Baroda aside, Indian Overseas Bank, Syndicate Bank and, to a lesser extent, Canara Bank give some of the pretentious private sector banks a run for their money.
- Likewise, all MNCs are not keeping their customers happy: Standard Chartered not only lags its MNC peers on most counts, it ranks 16th on 'service quality' in the overall rankings.

ROLE OF TECHNOLOGY

The Internet is the fastest emerging medium of transmitting of messages between banks and their customers. To this effect, the communication process of banking sector has changed a lot in the recent years. The RBI established the Indian Financial Network System, which is an efficient, and cost-effective communication system for banking. The payment system, which is the lifeline of banking, has benefited the most from the INFINET system. To make the fund transfer system safe and efficient, the RBI has added a new application system: Structured Financial Messaging Solution (SFMS). To take advantage of these systems, banks need adequate computerization, software etc. But most of the banks lack these facilities. They are merely concentrating on back office mechanization, which may not provide any value-addition.

Banking today requires decision-making on the basis of empirical data, and in an information age, it is essential that information management uses the best available means to transfer information on a real time basis. The INFINET provides for this and the infrastructure built up for this purpose is best utilized by the members of the INFINET Closed User Group.

Traditionally, payment systems in India have been individual scattered clusters with a substantial quantum of payments being routed through the non-bank based sectors too. With increasing concern over the existing state of payment and settlement systems in India, the RBI has taken up the cause for the establishment of an integrated payment and settlement system to benefit all the sectors of the economy apart from the common man at large.

Most of the payment system initiatives undertaken by the RBI are fairly well known. Apart from the existing facilities such as the Magnetic Ink Character Recognition (MICR) based cheque clearing, Electronic Clearing Services and the Electronic Fund Transfers, the Centralized Funds Management System, the Centralized Public Debt Office project comprising the Negotiated Dealing System and the Securities Settlement System, the introduction of Real Time Gross Settlement System are a few other products which would fructify in the near future.

Box 1: Banking Innovations – Does CRM Qualify?

Regulation and technological improvements are responsible for the vast majority of innovations in banking over the past quarter century. The introduction of personal computers and the proliferation of ATMs in the 1970s captured bank management's attention. The regulatory changes in the 1980s fueled much of the industry's growth, then downsizing as bankers focused on amassing market presence which resulted in significant merger activity. Recent technological improvements are at the root of bankers' focus as well as a target for their significant investment dollars today. In fact, according to recent projections, bankers and their financial service company brethren will spend almost $7 billion this year on CRM and increase that by 14 percent each year for the next several years.

Looking at this CRM phenomenon in light of the drivers of banking innovation since the 1970s, one might wonder if CRM itself is the innovation, or (conversely) the technology, once again.

Much is being written about CRM. Bankers at all points of the CRM spectrum are looking for a way to quantify their return on investment – either what it actually is or, if just starting out, what it should be and over what period of time should the value be realized. Ironically, the answer to this question may lie in a simple review of a few known quantities generated from historical innovation.

Look, for example, at ATMs. What drove many bankers to invest in ATMs was the promise of reduced branch cost, since customers would use them instead of a branch to transact business. But what was discovered is that the financial impact of ATMs is a marginal increase in fee income substantially offset by the cost of significant increases in the number of customer transactions. The value proposition, however, was a significant increase in that intangible called customer satisfaction. The increase in customer satisfaction has translated to loyalty that resulted in higher customer retention and growing franchise value.

Guess what? Internet banking, a product of the 1990s, shows similar characteristics. Again, bankers invested believing that the Internet was a lower-cost delivery channel and a way to increase sales. Studies have now shown, however, that the primary value of offering Internet banking services lies in the increased retention of highly valued customer segments. Again, the intangible called customer satisfaction drives the value proposition.

Now, we explore CRM. CRM is not another ATM or Internet bank. It is not a checking account, a stock or a mortgage. In fact, CRM is not anything a customer should even know about! You will never sell your customer your CRM, will you? So, one can conclude that CRM is not tangible. If it's intangible, can it be expected to produce a tangible return? Probably not, or at least not with any direct financial value exclusively linked back to the investment in CRM.

Is CRM another innovation, or the result of innovation? I think both. CRM is primarily driven by the innovation of technology, but unlike other technological innovations, CRM has the power to help bankers quickly and directly improve customer satisfaction. CRM is an added dimension to ensure that what the customer expects is consistent with what the bank is prepared to deliver. One expert in bank CRM initiatives recently said that CRM is an approach that is less focused on providing the right services to the customer than attracting customers who are the right fit for what the bank has to offer. Further, the primary value of CRM is its potential as a customer retention tool. People are starting to measure CRM in terms of increased customer satisfaction rather than ROI.

So, how much of a return can you expect from your CRM investment, and when can you expect it? Refer to your reasons for continuing to offer ATM and Internet banking services. The answer for CRM is the same.

Source: http://www.crm2day.com

SIGNIFICANCE OF COMPUTERIZATION IN BANKS

A great deal has been done in the form of computerization of at least the major branches at the commercially important centers. Even where computerization exists, there are varied platforms across even different branches of banks. The need therefore of the hour is to integrate computerization efforts, running parallel with business process re-engineering. In the absence of changes in work procedures, the benefits of mechanization and introduction of computers would not fully accrue to banks. Computerization without accompanying changes in work processes may perhaps result in increase in the work processes since there may be duplication at some levels resulting in no real improvement in the efficiency to banks. Further, mere computerization generally has been till now concentrating on back office mechanization, which may not provide any value addition to the ultimate customer who is the main reason for its business.

Yet another area, which is worth mentioning, is the relative slow progress in the establishment of bank gateways and connectivity to the INFINET for the critical common interbank applications, which are being implemented by the RBI. All the public sector banks must join the select group of INFINET members who would be among the first lot of users to exploit the benefits of the projects implemented by the Central Bank on a war footing.

Any Time Banking

Any Time Banking enables the customer to bank online 24 hours a day, seven days a week. ATMs are another type in the same category. In fact people started calling ATMs as Any Time Money machines rather than Automated Teller Machines as they are originally known to be. In this type of anytime banking, the customer is provided with an ATM card, which is an electronic card with few sensors embedded on it. When the customer inserts his card into the ATM it checks for the authorization and asks for the Personal Identification Number (PIN), which is known only to him. After the customer types his PIN, the ATM provides access to a range of services.

Some of the features in Any Time Banking are:

- Check account balances
- View account activity/account summary
- Transfer money between accounts (regular and recurring transfers)
- Make loan payments
- Place a stop payment on a check
- Reorder checks
- Export transaction history
- View check images.

Anywhere Banking

Anywhere banking is revolutionizing the way we live in. It is the mechanism of accessing our accounts from anywhere in the world. This is made possible by interconnecting the bank branches and the respective ATMs – thus making possible the use of one bank's ATM card with another bank's ATM through the use of a network system called as Shared Payment Network System (SPNS). As suggested by the Ranagarajan Committee, ATMs are being set-up in almost all areas such as shopping complexes, theaters, offices, complexes, airports etc., for the convenience of the customers. In addition, Any Time Banking provides another advantage of being geographically separated from the bank branch that operates the account of the customer.

Home Banking

The Internet, World Wide Web, Intranets, and Extranets are creating new IT infrastructures for all types of businesses. For banks, they are also presenting new business opportunities. Home banking, financial planning, asset management, bill payment, and other tailored customer services are just some of the products and services that will capitalize on the Internet's ability to reach customers.

There has been substantial progress recently in home banking and bill paying applications. Home banking bill payment began in the 1980s with some major efforts from various financial institutions. Banks view it as a method to lock in customers, and to increase the share of customer wallet retained by a financial institution. However, home banking bill payment has had limited success. Since its introduction, it has grown to about 3 + million regular users today.

HOME BANKING BILL PAYING

The consumer gives a payment instruction to his institution or to the bill payment provider directly. This payment instruction is then converted, or fulfilled, into a payment of one of a variety of forms, including ACH, paper checks, or unsigned demand drafts. In actuality, the payment instruction is often converted into two transactions – the removal of funds from the customer's account (disbursement), and the payment to the payee. Most disbursements happen electronically. As home banking bill paying has evolved over time, an increasing number of institutions have offered it to their customers. In actual practice however, the vast majority of these financial institutions do not process the transactions themselves, rather they outsource the transaction fulfillment process to one of a very few providers.

Corporate Banking

As businesses have become more efficient internally and have embraced such ideas as enterprise resource planning, it has become even more critical for financial institutions to provide services that support the new corporate culture. While credit remains a key determinant in bank relationships, delivery of fee-based services and information to commercial clients is of increasing strategic importance. Financial institutions that make right investment decisions and use technology appropriately will gain customer retention and rewarding relationships. Corporate banking provides basic banking services that companies need in order to operate.

The primary goal of a bank, which offers this facility, is to help clients create real competitive advantage through a blend of appropriate services and consistent experience. These result in better long-term strategic technology decisions and success. These include lending them money, investing the money they already have, and collecting and making payments on their behalf. It is sometimes known as institutional banking or relationship banking.

Businesses of all sizes rely on corporate banking. A very important aspect of corporate banking is to provide consistent services across borders for companies operating in more than one country. The services offered are quite complex in nature when the companies operate in more than one country. Some of them are:

- Managing a company's short-term holdings of cash, as well as funds held for longer periods; these are often invested in interest-earning accounts designed to maximize returns.
- Handling foreign currency and hedging against changes in its value by buying appropriate foreign exchange contracts.
- Financing imports and exports, including export credit arrangements.
- Transmission and receipt of money.
- Financing company projects, or purchases, or leasing of equipment; financing is often structured in complicated ways, for example, to minimize tax.

A payment service enables companies to make a one-off, same day payment, or regular payments to a large number of people or businesses, ranging from payroll services, to distributing share dividends, to settling trade debts. Corporate bankers sometimes have expertise in specialized areas such as emerging markets or shipping finance. They can also be involved in raising money in the capital markets by issuing shares and bonds, or through syndicated loans where the lending is shared by a number of banks. Efficient transaction processing, reliable financial information and good clearing services are at the heart of corporate banking.

Mobile Banking

Mobile communication devices are revolutionizing banking transactions over wireless networks and the Internet. To attract and retain customers, banks need to extend their full range of services across a wide range of mobile, wireless devices without having an impact on their current infrastructure and delivery channels it currently supports. Wireless networks, mobile gateways all play an important role in bringing mobile banking strategy to the market.

Mobile networks provide the following competitive advantage:

- **Always on 24 x 7 accesses:** Mobile networks enable consumers to be transaction-ready much in a way cable access has facilitated online PC access and reduced consumer dial-up delays.
- **Advanced penetration of mobile networks:** The 2G networks already cover more than 90% of the population in the western world and this number is growing steadily.
- **Personalization:** Through Subscriber Identity Module (SIM) cards, mobile customers have a specific profile that enables customized functionality to directly reflect the way they want to transact business over mobile devices. Through the convenient addition of a multi-application relationship card, mobile customers will also have a built-in platform for a host of other application services, including security keys, virtual credit cards and other customized payment instruments.
- **WAP** Rapid evolution of global protocols such as Wireless Application Protocol (WAP) enables the communication channel between computers and mobile devices. The WAP component essentially provides the facility for reformatting data for display in wireless handsets.
- **Faster data processing speed:** Increases in bandwidth and data transmission speeds make mobile data services efficient and cost-effective in a real time environment.
- **Security:** In addition to aforementioned smart card, a private key stored on the SIM card can protect e-banking transactions. Effectively, the mobile phone can become a wireless wallet to protect proprietary purchase and financial information.

MOBILE PAYMENT

It means executing a payment transaction using a wireless device, for example, mobile phone or personal digital assistant. The mobile device becomes the electronic payments device. Its mobility is its big advantage: it enables payments to be transacted regardless of place and time and for both bricks and mortar and Internet purchases. Announcements about new mobile payment solutions appear regularly at the moment. Potential players form partnerships and fight to win a place in Mobile Payment. These players include mobile operators, banks, credit card companies, mobile device manufacturers, smartcard manufacturers and a whole range of mobile payment start-ups.

Existing mobile payment solutions are based on one of these three distinct payment options:

i. Prepaid

ii. Direct from credit card or current account

iii. Paid through Phone bill.

SECURITY

The mobile phone should ensure the security of all personal data transmitted through the wireless handset to become transactional device. Just as e-commerce over fixed-line Internet device can hardly be expected to flourish if fraud or theft is easy business so also the consumer, subscriber, commercial entities and industry are unlikely to make full use of the potential of the new mobile communication media if they are insecure. Although security is mainly a matter of technology, there are two other important aspects – legal protection and customer perception.

TECHNOLOGY

Within the next few months, some real improvements will appear in the security of mobile payment technology platforms. When analyzing the security of a mobile payment transaction, we have to consider three distinct areas: the buyer, the medium between buyer and seller, and the seller.

- Security on the buyer's side implies security of the access device. Because a mobile device belongs to an individual, it is inherently more secure than a shared device. Solutions such as PKI and SIM2 will be introduced in the market early in 2001, which will significantly improve security for buyers.
- Real improvement in the security of the medium between buyer and seller will occur when 3G networks become operational. These 3G networks are based on technology that uses complex encoding and decoding algorithms, originally developed by the military.
- On the seller's side, acceptable levels of security will also be available in early 2001 when Wireless Transport Layer Security will be introduced. WTLS is an encryption technology, which makes sure that the seller receives everything sent by the buyer. A similar technology, TLS is currently used successfully in fixed-line e-commerce.

NEW TRENDS IN SMART CARD MOBILE BANKING

Smart card integration is also likely to play a vital role in driving new security standards for mobile banking, one which is based on existing banking relationship card models. By incorporating smart cards into mobile banking equation, e-banking customers will have a convenient, secure storage mechanism for retaining proprietary customer information, payment instructions, PIN numbers and in the most advanced scenario, digital signatures and private keys for PKI-based security. Smart cards also provide the opportunity to build an incremental revenue stream by providing an ideal platform, for extended applications and services. The emergence of multi-application relationship cards is destined to have an enormous impact on the mobile banking environment, alleviating security concerns while deriving customer loyalty.

For global financial institutions, the question is simply one of mobile or traditional channels. To ensure growth of consumer and corporate banking market share, a multi-channel delivery scenario incorporates customers' preferred channels for banking and provides an application framework of migrating to new channels as they come online. The mobile delivery channel is the latest of these and is preceded historically by branch banking; call centers, ATMs and e-banking. Multi-channel delivery also facilitates customer relationship management by integrating more seamlessly within customers' preferred business processes and financial management practices. Mobile networks can bring banks to a new level of service delivery by integrating completely and ubiquitously with every facet of customer life, and financial management decisions that are made at strategic points on route.

Financial institutions already have a flexible channel infrastructure supporting e-banking. Investment in mobile banking does not represent a technology leap that approaches the chasm between the real world and the virtual world. Meridian estimates that technology outlays required for implementing a mobile solution range is between USD 200000 and 300000 for average institutions since the technology investments represent enhancements and modifications rather than ground floor solutions.

Box 2: The Skinny on Fraud: Banks Aren't that Helpful When it Hits

Telephone and Internet banking afford consumers bill payment and purchasing conveniences at a time when most are desperately seeking an eighth day in the week. Time is so precious that most people can't live without such technological capabilities – who remembers paying every bill by hand? The price of this convenience: a greater likelihood that someday, somehow a consumer will be affected directly by fraud-much of it the work of bank insiders or those with access to customers' checking account information.

No problem, right? Wrong. While banks have spent scads of dollars educating the public on fraud, there's a disconnect between what banks intend to do on behalf of customers and what actually occurs once fraud is reported. And it's costing banks millions – not just in terms of fraud, but lost business because frustrated customers walk when they get little assistance in resolving such matters.

Take the experience of one customer at a top five US retail bank. While reviewing her bank statement on-line recently, she detected a series of unauthorized debits from her checking account to a merchant with whom she doesn't do business. Concerned these checks were fraudulent, she clicked to view the actual checks. What appeared were three checks, all bearing the names of unknown individuals.

A call to the bank's fraud department recorded the alleged crime, but the customer was told the account could not be closed until an investigation was completed. "What does that entail? They can still tap my account," the customer asked. "You must fill out an affidavit. We can't do anything until that is returned to us. Hold on and I'll get someone to assist you with a new account opening," the fraud specialist said. The new account person did assign the customer a new account, but no monies were transferred because that also requires a package of materials to be signed, plus the investigation must be closed, bank employees said. Both packages would be sent by postal mail. So, the customer waited-out her money ($685 at the outset) and with little confidence the package and affidavit would stop the thieves from striking again.

They did. By the time the packages arrived – one with new account information and the other bearing an affidavit for each unauthorized transaction, which all must be notarized and assigned a police report number – two more unauthorized debits had occurred. After four weeks, three phone calls to the fraud unit, three trips to the branch, one visit to the police department, and 12 different employees telling her 12 different things about the bank's fraud policy, the customer neither has gained access to her new account, nor recovered her stolen funds.

Source: http://www.banktechnews.com

FINANCE PORTALS FOR THE BANKING INDUSTRY

Banks are transforming their websites into finance portals. Finance portals offer strategic and operative benefits giving an opportunity for banks to offer personalized services to their customers on a one-to-one basis. By establishing effective finance portals banks can build long-lasting customer relationships, larger customer base and higher customer loyalty. Finance portals are becoming the interface between banks and their existing and potential customers. Portals serve as an all-in-one solution aggregating contents, services and commerce.

Banks are employing a variety of strategies to launch their portals. Banks using finance portals achieve strategic and operative benefits. The key strategic benefit is improved customer relationship, achieved through better service driven by deeper customer intelligence. Operative benefits include cross-selling opportunities and cost digression from off-to-online service.

The strategic benefit of finance portals lies in the management of customer relationships online, through which the bank can improve its image, get detailed data about customers and create single-customer profiles including their changing preferences. The management of customer relationships by getting and processing customer data is the key factor in protecting and improving a bank's core competencies. The key to acquire customer data is building and maintaining a successful portal; one that binds existing customers to the bank and attracts new ones.

The operative benefits of finance portals are derived from the business generated by the products and services offered. The most important operative benefit arises from internal cost digression effects resulting from the migration of offline to online handled transactions. The winding up of products/services like transfers or stock orders online can have a cost digression effect of 10 and more compared to offline.

Having determined the strategy, the bank must identify the target groups of the portal. Most finance portals differentiate three levels of users: visitors, members and bank customers. Visitors can access general information like stock quotes; members use additional services chat rooms or newsletters, and bank customers have access to all services, including online banking and real time quotes. With the strategy and the customer targets defined, portal construction can begin. Building a finance portal is a complex project, involving a variety of activities from web design to enabling online banking transactions to content management. The set-up and co-ordination of the project teams, normally including bank employees, consultants, partner companies and IT integrators, require to manage people with multi-disciplinary skills and diverse cultural backgrounds.

There are four components of portals. These are:

i. **User Interface:** To provide an attractive and efficient user interface, the Look and Feel of the website should provide the customer with a structured and simple view. The design should reflect the company's corporate identity to strengthen the bank brand online. Most importantly the Look and Feel should give the customer the impression that he acts in a secure environment and that the protection of his data is guaranteed by the bank. Navigation refers to portal's ease-of-use. It has to be intuitive and transparent, so that the customer always knows where he is on the website and how he got there. There should not be more than three layers of information, or more than three steps to get it. Last but not the least, online customers do not want to wait for information or for transactions to be completed. Performance of the website is a technology-driven issue, ensuring that even a customer with a low-speed Internet spends minimum amount of time. To guarantee fast connection to both high-and-low-speed users, some Internet sites offer high-and-low bandwidth access.

ii. **Contents and Services:** It comprises the information and transactions the customer can obtain or conduct on the portal – like the contents and services that offered depend on target customers' needs and can have a horizontal or vertical focus. The Products and Services offered on the portal, such as online banking, credits, even travel are also driven by the bank's target customer groups. Information about the Products and Service offered and in related areas of interest must be available to bind the customer to the portal. Thus, some portals have a NEWS section to attract and entertain the customer day-after-day. The finance portal also requires Interaction Tools enabling the

customer to stimulate the experience of the products/service offered. The integration and maintenance of these modules for customer's other areas of interest and other channels should be handled primarily by partner companies with relevant competencies. Another element of Content and Services component is the set-up of communities providing communication platforms such as forums in the bank customers' areas of interest. Furthermore, value-added services like free e-mail, SMS and WAP should be included to enable access to the portal via different communication devices. Help services provide customer support by offering FAQs, site maps, search engines, online-guided support and one-on-one chats among others.

iii. **Backend Transaction:** It provides interface for connecting the bank's legacy systems to handle online transactions, and integrates the online products and service with the banks' existing business processes. To provide online products and services to the customer, there has to be a connection to establish business processes. To reduce the complexity of the technical partner integration process, the partners should handle order-processing and fulfillment. Customer service support needs to be expanded into a web-enabled call center that can handle inquiries over the phone and the web.

iv. **Enabling Functions:** It includes partner management, marketing and quality assurance. Partner management deals with the screening, selection, implementation and development of partner activities as well as contracting, billing and conflict management. Marketing should focus on the marketing plan for introducing the portal and establishing the bank's brand as both an offline and online e-brand. It should also include internal communications for optimizing integration of the finance portal with existing business processes.

The Dynamics of Relaunches

They are necessary to keep the offering aligned with customer needs and technological innovations, and ahead of competitors' activities. Relaunches involve the addition of new products or services to the portal or the integration of new functionalities like games or quizzes. A relaunch may be necessary to adapt the portal to new technologies like General Packet Radio Service (GPRS) or Universal Mobile Telecommunication Systems (UMTS), which will enable access to multimedia information on a mobile telephone network. Relaunches should be communicated to keep customers informed about the portal development. Modifications or developments undertaken in a relaunch should be managed like the portal construction process. They require a holistic view of the finance portal and should therefore be coordinated by using the framework for finance portals.

Finance portals offer strategic and operative benefits, including the opportunity to establish a one-on-one relationship with each customer by providing personalized services on a direct-response basis, and internal cost digressions. Management of customer relationships is the strategic advantage of finance portals. It requires more information about each customer and more effective processing of that information to develop specific solutions for them. The outcome is a larger customer base and higher customer loyalty.

The key components of finance portals comprise a framework to manage implementation. Relaunches are a key component in the maintenance of the portal, ensuring it is always up to date vis-à-vis customer needs, technological developments and competitors' moves. Building and maintaining finance portals is a time-critical task for the banks, since a range of new entrants, some non-or-near banks are emerging. To achieve the necessary speed for portal building and relaunch requires enthusiastic people with multidisciplinary skills, because they not only need the specialist knowledge to build a portal, they also need to be able to understand quickly and play successfully according to the new e-rules.

Online Banking

Several banks have entered into online banking in an attempt to cut costs and attract new customers. However, in spite of heavy investments, the online initiatives of most banks are unprofitable. Moreover, the online channel has proved to be extremely expensive to develop and operate. It was just few years ago, that the Internet first beckoned to the banking industry, promising the world. The dream was vivid and seductive: The online channel would provide a cost-cutting engine more powerful than bankers had dared ever hope for; it would create new profits by bringing in legions of new customers; it might even develop into a robust new business itself. But the dream for many financial institutions has turned into something of a nightmare, not only has the online channel proved extremely expensive to develop and operate, it has not enabled significant cost cut elsewhere. While banks have enrolled some existing customers in their online programs, droves of new ones simply have not appeared. Despite billions spent, the online offerings of most institutions remain unprofitable. Many have started to question whether there is value in the online channel after all. In fact, the value is there. It is just that banks, for a small minority that are ahead of the curve, have been suing wrong means to extract it. Enrolling customers in online programs is a good start, but it only adds cost if they do not actively use the site. Investing in fancy functionality can be counterproductive, since usability and security are what customers want most. The main drivers of value in the online channel – cost reduction, cross-selling opportunities and higher retention – will never be optimized until institutions can significantly increase site usage and effectively coordinate the channel with branches and call centers.

The bottom line is that banks must activate their online customers and integrate the new channel with traditional ones. This is winning proposition of the future. Moreover doing so, financial institutions can actually reduce their technology expenses by redirecting them towards the 20% of online initiatives that bring 80% of the value.

People who are not active online clearly represent the vast majority of banking customers. And they have rational reasons for staying offline. Typical laments including feeling intimidated by the site and uncertainty over the value proposition – in other words, “why bother?”. There are also lingering concerns about security and frequent complaints that signing up is complicated and time-consuming.

Financial institutions can counter these forces by refocusing investment on improving the site’s basic functionality and user-friendliness and by avoiding costly endeavors that most people neither understand nor value. For example, banks have invested heavily in a host of peripheral projects such as aggregation with little or no return. The truth is that developing advanced capabilities that appeal to a relative handful of customers creates far less value than strengthening core capabilities and getting people to sue them. Indeed, institutions must follow up this redirection of investment by pushing relentlessly to familiarize customers with their sites and by showing people how easy and efficient the online channel is to use. Pricing should encourage migration online and registration should be simple.

BCG’s research suggests that roughly 80% of the online channel’s potential value can be realized by implementing these initiatives, plus a handful of others such as developing retail and commercial online lending facilities. By concentrating on the basics, banks can cut costs substantially now. There are moreover, specific ways to approach these tasks. When people struggle mightily to execute what may strike as elementary transactions, take it as a sign that the site needs redesigning. And make the design process user-driven – customers should be involved at every stage. It is their comprehension, not that of a technology-savvy few, that is important. Above all, keep things as clear and simple as possible. A home page that lists everything a bank does is more overwhelming than helpful.

Banks can also stimulate usage by marketing to consumers personally. When customers contact the call center to request a transaction, a representative should mention that the task is easily done on the web and ask whether the customer would like to be walked through the process or register. Internet equipped road show kiosks can periodically be placed in branches where staff is available to explain to curious customers how basic transactions are carried out. In promising online usage, banks need to think in mass-market terms but keep in mind that people come aboard one by one. It is a grinding unglamorous work, but the potential benefits are substantial.

Achieving high-levels of activation will go a long way towards optimizing the value of the online channel. But there is another big piece of the puzzle: integrating the new channel with the rest of the bank. This is critical because nearly all the value of the online channel is realized offline – in cross sales completed in other channels and in cost reductions. It is vital that investments in the online channel be tied to commitments to capture the benefits online. An actively used online channel should thus serve as a conduit to the branch staff, the call center and the relationship manager. The focus must be on smooth hand offs because integrated channels working together are far more effective than a group of silo-like entities working principally alone.

To engender this integration it helps to formulate paths that people in various customer segments are likely to take among channels. The interactions in each channel can then be fashioned around the paths. For example, a relationship manager needs to think about which channels the customer used before coming to her and which channels the customer is likely to visit next. Each venue must have entry and exit activities designed to welcome customers and then send them on to still other channels. The goal is a seamless multi-channel experience. The knowledge a customer shares between the channels is the key. And banks that effectively meet this challenge will create an environment in which everybody wins: the customers by being given multiple linked ways to search out the financial services they need; and the institutions themselves, by being there to deliver those services.

Call Center Banking

Traditional banking meant offering mass products like deposits and loans. But with the advent of computerization, globalization and innovation in technology there were a lot changes made to the traditional banking. These changes were mainly seen in the era of ’90s.

Call center may be defined as a central place where the customer and other telephone calls are handled by an organization, usually with some amount of computer automation.

Once viewed as a low-cost alternative to branch banking and a necessary cost to provide customer service beyond the regular working hours, call centers today are increasingly important in helping an organization meet their challenges. They mainly include maximizing returns through customer contacts and deliver superior service while maintaining costs. A World class call center is:

- Aligned with business strategy and direction
- Customer centric
- Seamless in providing channel parity
- Flexible, effective and efficient in operational structure
- Lean in management structure
- Robust in infrastructure, support and service recovery
- Capable of attracting and retaining talented staff who can deliver on service promise
- Enabled by a technology solution.

Call centers are fast emerging as the central resource supporting all contacts with customers, regardless of access channel. Customer service will evolve to meet customer requirements.

Call centers are where customer service executives are present to answer, respond and solve customer queries over the phone. Usually these call centers function round the clock providing, 24 × 7 service to the customers. Though, most of the banks that have a presence in various time zones in the world, most Indian banks still have only daytime call centers. Apart from resolving queries, the call center agents' work includes, for example, handling responses to an advertising campaign, or calling existing customers to offer additional services. This type of marketing of services is also called telemarketing. A call center is basically a communication center that has the state of the art telecom facilities, which are manned by trained customer service executives to provide the necessary support to the customers. The primary focus of call center banking is providing service for basic account transactions like balance enquiry, requests for Cheque books and other queries such as loss of an ATM PIN code etc. Another area of use is the marketing of finance products such as loans, term deposits and other financial services.

BENEFITS OF A CALL CENTER

- Enhances the customer base and business prospects.
- Offers an economical means of reaching diverse and widely distributed customer group.
- Fine-tunes offerings to specific customer groups by specialized and focused assistance.
- Allows customers easy access to experts.
- Facilitates business round the clock and in any geographical region.
- Allows a company to reduce the overheads of brick and mortar branches.

CALL CENTER CLASSIFICATION

- Voice call center with phones and computers.
- E-mail call center with leased lines and computers.
- Web-based call centers that use Internet chat facilities with customers.
- Regional call centers that handle calls from local clients.
- Global call centers that handle calls from across the world.

CALL CENTER TERMINOLOGY

- **Automatic Call Distribution (ACD):** The ACD processes all inbound telephone calls on a first come, first served basis. The system answers each call immediately and if need be, holds it in a queue till the time an agent is available. When the agent becomes free he or she services the first caller in the queue. A system can be configured to offer different kinds of treatment to different callers. For example, people calling long distance can be given priority handling. Or calls from customers placing orders can be taken before than those seeking technical support. By providing sequencing and uniform distribution of incoming calls among multiple agents in a call center, ACDs offer time/labor savings and enhance productivity.
- **Interactive Voice Response (IVR):** IVR applications support the automated retrieval of stored data. These usually took the form of pre-stored messages saying 'press 1 for this or press 2 for that'. IVR applications range from basic inquiry to the most sophisticated speech recognition applications.
- **Computer Telephony (CT):** CT is one of the most common features of call center environments. They can either be a simple screen pop-up window, a sophisticated call control algorithm that can search for the last agent that

spoke to the caller, or a predictive dialing solution that doubles the efficiency of outbound calling. With a simple click of mouse, a call center agent can quickly move between a customer profile, product information, customer history, order entry, fulfillment request, template cover letters and quote entry, among other fields.

- **Web Integration:** The integration of web technology in call centers offers personalized, time and cost effective customer service. Organizations can either have a call back button on their web page whereby a call is automatically made to the customer or have a seamless addition of voice over IP to the web application.
- **Reporting Systems:** Different reporting applications are used to optimize the use of different communications platforms. Depending upon the firm's specifications, either simple proprietary tools could be used or advanced tools that blend information from multiple communications or information systems platforms can be adopted.
- **Work Flow Management Tools:** Coordinating telephony applications with information systems applications, workflow management tools assist call center supervisors to script and manage employee activity. For example, selecting the best agent for handling particular type of calls.

MULTI-CHANNEL OPERATIONS (REMOTE BANKING)

Technological advances have made it possible to offer banking products and services to customers through multiple channels. Some such services are: ATMs, phone banking, Internet banking, mobile banking, call centers, interactive TV, which have brought the customer closer; and the interaction is not limited to banking hours or brick-and-mortar structure. The customer intimacy had never been better. However, these channels have to be integrated to have a meaningful customer relationship. Multi-channels enable centralization of processes and diversion from branches, which are expensive. Transactional costs involved in channels are lower than transacting at branches. Branches are used to educate customers about products and other efficient channels of the bank because having all these channels is not enough; educating the customers with the right kind of information is necessary so that it removes mental blocks once the customer is aware of a channel. Number of customers using online banking is short of expectations worldover due to security concerns of educated but it is not so with the rightly educated customers. In addition, the security threats have to be genuinely addressed beyond just systems of security, by changing the mindset of employees towards security and through well-defined procedures in place. Customers are able to reach the bank anytime of the day from the place of their choice and open a new account within minutes and can access information. Once customers have the information readily available, they can switch banks at will and loyalty is not guaranteed.

Automated Teller Machines

The spread of ATMs is such that the SBI has placed an order of 1500 ATMs with NCR Corporation. The NCR alone has installed 8700 ATMs in India at the end of March 2003 and the number might cross the 10000 mark considering the SBI order. The next level of ATMs are also coming up in a big way, these are the shared ATMs, where customers of different banks can access their account information and withdraw money and perform other functions at a single ATM. Access to customers of a bank would not be limited to the ATMs owned by it but the pool of all the ATMs of a set of banks would allow operations for all the customers of the group of banks.

ISSUES AND CHALLENGES FOR ATMs

Though ATMs have become one of the important channels of marketing and distribution, they themselves do not increase the customer base or the users of banking services or the volumes. United States saw an increase in number of ATMs from 139,000 to 324,000 in five years with disastrous results. The number of transactions per machine dwindled from 6,876 per machine in 1992 to 3,308 per machine in 2002. This situation might put pressure on the profitability of the ATMs. To counter this, banks have to look for additional revenues in the form of vending, ticket booking and other web-enabled services. To support these functions, banks need to procure Internet-protocol enabled ATMs that could be prohibitively expensive. Other possibility is to cut running cost by wireless technology. However, such widely networked ATMs could turnout to be a disadvantage during a crisis. The major problem is the logistics of delivering cash physically to all the ATMs. Banks need to have the right technology platform from where they can monitor and manage on real time basis, the cash position of each of the ATMs. Added to these, there is also a problem regarding increased complaints with the increase in the number of ATMs and also the unauthorized withdrawal methods that have become very complicated.

APPLICATIONS OF ATMs

- **Cash Withdrawals:** The basic purpose of ATMs is to provide a 24-hour unmanned teller, to meet round-the-clock money needs of the customers. Maybe due to this service, ATMs are popularly known as 'Any Time Money'. The withdrawals can be anytime at any place and from any machine.
- **Cash And Cheque Deposits:** Customers can deposit cash and cheque through an ATM anytime.
- **Information About Balance:** Customers can have an access to a wide range of information about their accounts such as balance, cheques credited and debited, bank charges for various items etc.
- **Ordering Cheque book:** Customers can order a cheque book anytime from ATM.
- **Ordering Bank Statements:** Customers can order Periodic bank statements through an ATM.
- **Direct Transfers:** Transfers can be of two types. They can be between different types of accounts belonging to one account holder or they can be between two different accounts of different holders.
- **Arrangements for Regular Payments:** Payments of telephone bills, insurance premium, electricity bills, periodical membership payments etc., can be easily handled through an ATM.
- **Issue of Travelers' Cheques:** ATMs can be used to issue travelers cheques of various denominations.
- **Handling of Loan Applications:** Although complete processing of a loan application is not possible on an ATM, certain basic formalities can be completed with its help.
- **Point of Sale Transaction:** ATMs can be used for POS transactions. Customers making purchases can pay through ATMs, which will directly debit their account and immediate credit will be given to the retailer's account.
- **Miscellaneous:** Banks offer a number of other services to their customers through ATMs. ATMs can accept share applications, and can also be used to buy and sell shares and other securities.

Para Banking

Banks of today are becoming more like Multi Brand Outlets having a Shop-In-Shop kind of structure of organized retail marketing. The multiple offerings are mutual fund units, insurance policies or anything that has cross-selling potential. A brand promoted for a particular product at a considerable cost draws thousands of customers. Retail banking, unlike corporate banking, has nothing to do with the customer relationship. It only deals with their behavior. The need is to create a brand, so that customers come into the bank.

Coffee Pub Banking

Coffee pub banking, which stands for relaxation, stimulation and enjoyment, is a new concept. Kasikornbank, Thailand's third largest bank has launched Asia's first coffee-banking service hall at its Bang Kapi branch in Bangkok. Sitting in a Starbucks coffee shop next door to the branch, Kasikornbank's customers can enjoy coffee and music while electronic board hails them to the counter. Of the 200 square metre branch, 70 sqm is dedicated to Starbucks. Kasikornbank and Starbucks share the rent. Both the parties have developed the branch design over an eight-month period. The Starbucks area is open from 8 am to 11 pm, with Kasikornbank services available from 8:30 am to 7 pm on week days.

E-lobby

E-Lobby provides 24-hour automated banking services, including ATM machines, phone banking, and Internet banking. Customers no longer have to rush down or wait in a long line during lunch break. They can come to bank anytime or even at the weekend. This concept increases customer convenience and satisfaction. It also shows customers that the banks care for them.

Mobile Vans

Teams with at least five to 10 staff could go out in a van and set-up a booth in various localities, offices and villages offering consultation on personal finance issues related to the bank's products. There would be a mobile bank right in front of door. Standard Chartered Nakornthon Bank of Thailand has launched such mobile teams into Bangkok's communities, offices and villages.

Narrow Banking

One form of narrow banking is investment in short-term safe assets and other one is a bank to extend credit to small firms. The recent trend in banking regulation discussions concerns the question of how to prevent contagion in the financial system. Bank regulation thus far has been mainly dependent on a safety net such as deposit insurance. The crucial feature of a safety net is that it relies on the ex post discretionary intervention of the state. Lately it has been pointed out that while the stability of the financial system owes much to such a safety net, the latter has also generated social costs due to the moral hazard behavior of financial institutions. Thus an *ex ante* regulatory method based on market discipline is being sought to replace *ex post* discretionary regulation. Narrow banking proposals are being given attention because it is considered that may constitute one of the regulatory mechanisms that could replace discretionary regulation. The proposals are that two major functions of banks should be undertaken by different institutions in order to prevent contagion of financial risk via the payment system. Narrow banks are broadly defined as banks that specialize in deposit-taking/payment activities, while not being able to provide lending services. They are often cited as the banks that specialize in deposit/taking, payment activities and are prohibited from engaging in lending activities.

A CONCEPTUAL CLASSIFICATION OF NARROW BANKING

Robert Litan's (1987) Proposal

The first narrow banking proposal in history was set forth by Professor Robert Litan. The proposal is that "financial holding companies" be authorized to become highly diversified financial conglomerates. These companies would have two kinds of subsidiaries: "banks" and separately incorporated lending subsidiaries. The banks would serve as transaction processors, accepting deposits and investing only in highly liquid safe securities or in practice, obligations of the United States Treasury or other federally guaranteed instruments. On the other hand, the financial holding companies would extend lending services only through their lending subsidiaries wholly funded by commercial paper, debentures and equity etc.

Pierce's Proposal

Professor James Pierce designed this proposal. It separates monetary and financial functions into individual institutions. While monetary service companies fulfill the monetary function, financial service companies handle the financial function. Monetary service companies provide checking accounts and wire transfers and are permitted to pay interest on all their accounts. But the extent of the assets that they can hold is restricted. That is, the assets are limited to purchases of the kind of short-term, highly marketable and highly rated instruments that are in the portfolios of today's money market mutual funds, such as short-term treasury securities, and highly rated commercial papers. The monetary service companies correspond to narrow banks and provide payment services, including check clearing, electronic funds transfer, and discount windows. On the other hand, financial service companies can conduct all other activities, including insurance and retail banking.

Bryan's Proposal

Lowell Bryan of Mckinsey has designed this proposal. In this proposal, a financial holding company is established and the bank subsidiary fulfills narrow banking function. The extent of the safe assets the bank subsidiary can hold is broad – some of the lending services such as mortgage loans can be provided by the bank subsidiary; hence the bank subsidiary in this proposal is engaged in credit creation. The lending subsidiary on the other hand, provides such services as highly leveraged transactions and LDC lending.

To summarize, one proposal allows the narrow bank to invest only in short-term safe assets such as treasury bonds (Pierce's Proposal) while the other proposal allows the bank to extend credit to small firms (Bryan's Proposal). In other words, there is no uniform definition of a narrow bank as regards its range of functions. This difference in defining narrow banking activities leads us to question how robust each proposal would be in protecting against financial risk and what kind of proposal is more effective for maintaining the stability of the financial system.

It is worth mentioning that some argue that the primary reason behind the combination of these two activities is the existence of financial regulation, rather than synergy effect. Banks have a natural tendency to prefer a fund, which is covered by deposit insurance, causing moral hazard to prevail. In order to obviate the banks' moral hazard problem, it is better to separate deposit taking and lending activities into different institutions. Thus, narrow banking proposals such as those of Pierce and Litan are supported. Another view, which stresses the existence of this synergy effect, finds that the Pierce-Litan type of narrow banking is a source of inefficiency. They stress that the core activity on the banks' assets side is to provide a commitment line of service to their customers. The commitment line has similar features to those of a demand deposit, since customers have free access to liquidity up to an amount specified in advance. Consider the following two situations; first, the liquid asset is owned by a single bank which takes care of the liquidity needs on both the assets owned by two separate banks, one of which deals with the liquidity need of the asset side while the other deals with the need on the

liability side. The welfare level of the former seems to be higher than the welfare level of the latter. This seems to suggest that the narrow banking proposal submitted by Bryan who claims that the two activities should be provided at the same institution, is supported.

Offshore Banking

Financial experts have been pleading to establish an offshore banking center in India. One of the significant features of the Exim policy is the proposal to permit offshore banking units in Special Economic Zones. Offshore Banking refers to the International Banking business involving non-resident foreign currency-denominated assets and liabilities. It refers to the banking operations that cover only non-residents and does not include domestic banking. An offshore banking center is a place where deliberate attempt is made to attract international banking by offering many concessions in the form of taxes and levies imposed at lower rates. A more important relaxation is the exemption of the offshore banks from restrictions on operations. Offshore banking units in these centers can carry on their activities with international enterprises or investors without conflicting with the domestic fiscal and monetary policy.

Offshore banking centers offer the following benefits:

i. Exemption from minimum reserve requirements.

ii. Freedom from control on interest rates

iii. Low or non-existent taxes and levies.

iv. Entry is relatively easy, especially for large international banks, in contrast to the situation in neighboring countries that may strictly limit or prohibit the entry of foreign banks.

v. License fees are generally low.

vi. Close proximity to the important loan outlets or deposits sources.

Offshore banking is an extension of the euro-currency concept in the East, which provides a link between euro-currency markets and the final borrowers. They provide essential time zone links that are truly worldwide, and ensure that the market operates 24 hours a day. While offshore banking is an integral part of the euro-market what distinguishes it from the mainstream euro-market is that it was specially set-up by host countries to promote international banking. Offshore banking units are branches of international banks or other subsidiaries or affiliates. They do not carry retail business, but generally provide wholesale banking services, project financing, syndicated loans, issue of short-term and medium-term instruments such as negotiable certificates of deposits and capital notes as well as merchant banking activities in foreign currency denominating bonds and equity shares. The deals are mostly between banks or with large borrowers or Multinational Corporations. MNCs prefer transacting in offshore financial centers because of certain apparent advantages like avoidance of high tax incidence, freedom from exchange control, maintenance of secrecy of deals due to non-interference from government and regulatory authorities, and deferring tax by floating subsidiary units in such centers and delaying their remittance of profits to the parent company when it would be taxed. A few Indian Banks such as State Bank of India, Indian Overseas Bank, Bank of India and Bank of Baroda, have set-up offshore banking units for deposit taking and final lending at Bahrain, Hong Kong, Colombo, and so on. Indian Bank, Bank of Baroda and Union Bank of India jointly floated a deposit taking company, IBU International Finance, in Hong Kong for both offshore and onshore banking. The benefits for the Indian Banks from these ventures are:

i. Sizeable profits – as these ventures involve relatively low operating costs.

ii. With multi-currency deposit bases, the banks would be able to serve better the needs of their customers who have set-up joint ventures abroad in the form of foreign currency finance.

iii. The banks would strengthen the country's balance of payments through repatriation of profits from the venture.

OFFSHORE BANKING CENTER IN INDIA

Financial experts have been pleading to establish an offshore banking center in India. Geographically, India provides distinct advantages in attracting offshore banking units, because it has a stable economic and political performance, a vast market, technical manpower that could find employment in these centers. Another advantage is that the Indian market would open a little before the Tokyo market closes, and close before New York market opens, thus providing a vital time link for international money market dealers. In an era where many Indian corporations are functioning abroad and many corporations are granted permission to seek overseas finance, establishing an offshore unit will help tap the resources.

i. Exporters would benefit in terms of finer margins on loans and better foreign exchange rates available via an offshore banking unit. The benefits of multi-currency operations, which to an extent minimize currency fluctuation, will be an added advantage.

ii. Salaries paid by offshore banks and local expenditure incurred by them contribute to the economy's welfare. For smaller countries the benefit would be greater. For a larger country such as India, however, this may not form a significant portion of the total income.

iii. India may earn revenue in the form of license fees, profit taxes imposed on the banks operating in the area. It may also get the benefit of banks' funds in the form of capital and liquidity requirements.

iv. The country can gain improved access to the international capital markets.

v. The domestic financial system may become more efficient through increased competition and exposure of the domestic banks to the practices of offshore banks.

vi. The offshore banking centers will provide opportunities to train the local staff, which will in turn, contribute to faster economic growth.

vii. The offshore banking units would help channelize non-resident Indian investments.

viii. Setting up offshore banking centers would trigger enforced development of more advanced communication facilities, a must for their functioning.

But establishing offshore centers also comes with a price:

- The supervision and regulation of offshore banks may involve substantial costs.
- Encouraging offshore banking may result in the diminution in the autonomy of domestic monetary policy, since it is difficult to always draw a line between the offshore and onshore operations particularly in the absence of exchange control.
- Offshore banking provides scope for tax evasion by residents. For instance, in Hong Kong, it was found that residents place deposits with offshore banks and take loans of the same amount. The interest on deposits is not taxed.
- Offshore banks may prove to be harmful competitors to the local banks and may inhibit their growth.

Box 3: Waves of Changes

The first wave of change in banking technology came with the use of Advanced Ledger Posting Machines (ALPM) in the 1980s. The RBI advised all the banks to go in for massive computerization at the branch level. There were two options: automate the front office or back office. Many banks opted for automating front office ALPM in the first phase. Banks like State Bank of India concentrated on the back office automation at the branch level. The Rangarajan Committee Report of 1985 ensured that banks had to get computerized. With the second wave of development in late 1980s came Total Bank Automation (TBA). This automated both the front-end and back-end operations within the same branch. TBA comprised of total automation of a particular branch with its own database. In the third wave, the new private sector banks entered the field. These banks opted for a different model of having a single centralized database instead of having multiple databases for all their branches. This was possible due to the availability of good network infrastructure. In the beginning of the 1990s, leased line costs came down. The DoT expanded its capacity and new technologies were being implemented. Earlier banks were not confident of running the whole operation through a single datacenter. However, when a couple of private sector banks showed that it can be done efficiently, other banks began to show an interest, and they also began consolidating their databases into a single database. Banks followed up this move by choosing suitable application software that would support centralized operations. The fourth wave started with the evolution of the ATM delivery channel.

The second stage was Suvidha Experiment in Bangalore. This showed the power of technology and how the reach can be increased phenomenonally at a great place. Seeing these all the banks started revamping their retail delivery channels. Their core focus became the number of customers they can service at lower cost. The main channels were Internet Banking and Mobile Banking. After this came alliances for payment through various gateways.

The third important development happening now is the real-time settlement system of the RBI. Once this is in place, transactions between banks can be done through settlement system, online, electronically. So the collections will become very fast.

THE REGULATORY FRAMEWORK

In 1999, the RBI established the Indian Financial Network to offer an efficient cost-effective communication system to the banks. INFINET offered an effective fund transfer system called Structured Financial Messaging Solution to provide safe and efficient transfer of funds with the help of robust security features like a Public Key Infrastructure which utilized most advanced encryption technology. Banks need to have adequate computerization and software to use the services of INFINET. Other facilities include cheque clearing based on Magnetic Ink Character Recognizer, Electronic Clearing Services, Centralized Funds Management System, Electronic Funds Transfer, Securities Settlement System and Centralized Public Debt Office including Negotiated Dealing System. INFINET system also offered inert-city bank transfer facility to the banks.

In mid-2000, the RBI launched the Real Time Gross Settlement System to offer secure online fund transfers. The RTGS system helped in the transmission, procession and settlement of funds as per the customer's instructions on a constant basis. The system had various security levels such as 128-bit cryptography, access security technology, firewall technology etc. The RBI also took steps to enable inter-connectivity across banks worldwide.

In early 2001, the RBI issued guidelines for e-banking. These guidelines covered various issues that fall within the framework of technology, security standards and legal and regulatory issues. As per the guidelines, the existing banking regulatory framework also applied to e-banking and covers any entity involved in providing

online e-banking products and services to the residents of India. According to the RBI notification, banks should acquire prior approval to offer e-banking services and the banks that were already providing such services were required to acquire the RBI's post facto approval.

The RBI stipulated that virtual banks were not permitted to offer e-banking services in India and stated that only banks licensed under the Banking Regulation Act and having a physical presence in India were allowed to offer such services. The RBI clearly stated that e-banking should include only Indian currency and in case of cross-border transactions, the restriction would continue to apply unless permitted by FEMA.

The Indian government has approved the Cyber Bill and has promised to make amendments in the related laws like Indian Evidence Act, Criminal Procedure Code Act, Companies Act, Contract Act and the Indian Penal Code. The amendments would enable the courts to accept cyber contracts and documents sent over the Internet. This is expected to increase e-banking.

SUMMARY

- This chapter focuses on the facilities that have to be provided for rendering good customer service at low costs. Primarily, the banks have to rely on cost reduction exercise for this purpose.
- This chapter begins with an explanation about this exercise. Technology plays a crucial role in this exercise. Hence, the role of technology has been discussed.
- As part of using technology for implementing customer service programs, banks have computerized their branches in a large way and the significance of this step is discussed.
- Consequently, banks have started finance portals for multitude of services and details about various aspects have been covered.
- Also details about certain facets of banking like Narrow banking and Offshore banking that should give a good idea regarding the entire gamut of services for the customers have been covered.
- Aboveall, all the activities can be rendered effective only if activities are performed as per the regulations. Hence, the chapter ends with a discussion about the regulatory framework in the emerging era of e-banking.

Chapter VII

Payment and Settlement Systems

After reading this chapter, you will be conversant with:

- Payment Methods
- Electronic Fund Transfers
- Automatic Teller Machines
- Electronic Clearing Service
- Electronic Data Interchange
- Financial Networks in India
- Real-Time Gross Settlement Systems
- Digital Certificates

Consumers, businesses and individuals can pay for relatively small purchases, in several ways: they can pay with cash; they can transfer funds from a checking account using a check or, much less frequently, a debit card; or they can use a credit card to charge purchases against an established line of credit. Other forms of payment, except for cash, involve computer networks linking banks and other financial intermediaries. They make such payments more rapid and efficient.

PAYMENT METHODS

Traditional payment methods include cash, cheques, electronic fund transfers, and credit cards. Payment by cash means an immediate physical transfer of funds, unlike other methods of payment, which involve changing notations in the ledgers of financial institutions. Each method of payment differs in terms of the regulations covering it and the degree of privacy, anonymity, and protection it conveys to consumers.

Cash

Cash is defined as coin and currency (paper money). If cash is lost or stolen, the unlucky party suffers the loss. From the perspective of consumers and merchants, an instantaneous transfer of value occurs in cash transactions; thus, payment and payment finality (the merchant has the money in hand) are simultaneous. Anyone can accept cash as payment; cash transactions require no electronic readers or authorization networks.

The person or institution holding the cash bears the risk of theft or that it may be counterfeit. There is no security for the money held in cash.

Notational Money

Most money exists not as cash but as notations in the ledgers of depository institutions (banks and other financial institutions). Debiting one party's account and crediting another party's account execute notational money transactions. Depository institutions must be ready to convert notational checking deposits into cash on demand.

The Indian Government operates a system of deposit insurance that protects depositors against loss (Upto Rs.100,000 per insured account in an insured institution) if the depository institution fails. Thus, depositors are protected against the risk of losing all of their money on deposit.

Notational money transactions are generally not anonymous and consequently may not be completely private either. Banking laws protect the confidentiality of an individual's financial records when other parties seek access to them.

Payment by Cheques

The most common form of notational money is an account with cheque facility. A cheque is an order authorizing the transfer of money from one account to another; it is not a token that represents value, as cash does. When a cheque is accepted as payment, the recipient's bank collects the value of the cheque after presenting it to the bank on which it is drawn. Because a cheque can be returned for insufficient funds, the bank may not make the funds available to the recipient until the day a returned cheque would have been received – a lag of three days for local cheques and over five days for non-local cheques. Consequently, merchants who are paid with a cheque may have to wait several days before they receive their money.

The person who wrote the cheque can stop payment on it by notifying the bank that holds the account if a cheque is lost or stolen. Unlike counterfeit currency, however, the validity of a cheque cannot be determined by visual examination. A cheque may be worthless because it is counterfeit or because the cheque writer does not have sufficient funds in his or her account.

Apart from the normal cheques, there are **Banker's Cheques and Demand Drafts**, which are special kinds of cheques. A banker's cheque is drawn by a bank on its own funds. It is a direct obligation of the bank; individual consumers cannot write banker's cheques. A demand draft is guaranteed to be good by the bank on which it is drawn. A customer usually pays a fee to have a banker's cheque or DD. The payee of the banker's cheque/DD can be sure that it will be paid when presented. Both banker's cheques and DDs are considered insured deposits.

Traveller's cheques are also included in a bank's net transaction accounts and thus are subject to reserve requirements. Traveler's cheques issued by a bank are covered by deposit insurance, but traveller's cheques issued by a non-depository institution (such as American Express) are not.

Box 1: RBI Panel Wants Cheque Truncation in Four Metros

MUMBAI: A Reserve Bank of India constituted working group has recommended that cheque "truncation" should be introduced in four metros in the first phase due to the high volume of transactions.

Once the truncation process was established in these centers, rolling it out at other places would be a relatively easier task, the group said in its report. Cheque truncation is the process in which the physical movement of cheque is curtailed or eliminated by electronic records of their content for further processing and transmission.

The group, chaired by RBI Executive Director, R B Barman, has recommended that in India cheques should be truncated at the presenting bank itself and there should not be any amount-based restriction.

Referring to the mode of truncation, the panel has recommended an electronic image based model. It also said suggestion to change the existing statutory preservation period of eight years under "Banking Companies Preservation of Records" Rules 1985 to one year should be made to the government.

The group also considered that storage requirement of the electronic image of physical cheques and recommended that preservation period should be eight years.

From the point of view of efficiency and control, centralized agency per clearing location should act as an image warehousing facility for banks, the group noted.

However, given the challenges involved in setting up a single agency in the Indian context, the group recommends that the choice could be either a single agency or individual drawee bank as the points of storage, it added.

Truncation and standardization of cheque format should be independent initiatives with the latter being implemented even after the introduction of cheque truncation and therefore should be introduced in India for settlement to be generated on the basis of the current structure of the MICR fields, it said.

Public Key Infrastructure (PKI) should be adopted to protect data and image flow over the network. To establish authenticity, non-repudiation and integrity, it suggested that digital signatures should be used.

The group also recommended that the security requirements for the storage of images by the banks or the centralized warehousing agency should be in consonance with the requirements of the IT Act 2000.

Source: http://economictimes.indiatimes.com/articleshow/178751.cms

ELECTRONIC FUND TRANSFERS (EFTs)

Notational money can be transferred from one account to another or converted into cash through Electronic Fund Transfers (EFTs). Such transfers are initiated through an electronic terminal, telephone, computer, or magnetic tape to authorize a financial institution to debit or credit a consumer's deposit account. Examples of Electronic Fund Transfers include Point-of-Sale (POS) transfers using a debit card,

transfers at Automated Teller Machines (ATMs), and direct deposits or withdrawals made through an Automated Clearing House (ACHs).

The customer receives a written receipt when an electronic transfer is initiated and periodic statements describe each transfer. Electronic fund transfers leave an audit trail and are therefore not anonymous because of the requirements for receipts and periodic statements.

AUTOMATIC TELLER MACHINES (ATMs)

Modern industrial economies still function to a large extent on cash payments despite the development of electronic payment systems. Although cash payments represent the direct converse of electronic forms of payment, cash delivery is itself increasingly based on the huge base of Automatic Teller Machines (ATMs), which are being increasingly networked together to permit customers to collect cash from different banks as well as in other countries. ATM and credit card networks are linked in that VISA and MasterCard holders have long enjoyed the facility to draw cash from ATMs. ATM networks are increasingly being developed by non-banking organizations although originally established by large commercial banks. In the US, the company currently installing the most ATMs is Electronic Data Systems (EDS), a computer/data processing services company.

Plastic Money

Debit cards, Credit cards and Smart cards are collectively referred to as plastic money because they are made out of plastic. A brief description of each of them is given below.

DEBIT CARDS

The customer enters a personal identification number to authorize the transaction in a typical purchase using a debit card. The merchant's computer then requests authorization from the computer network usually the regional ATM network that links the merchant's bank with the customer's bank. The customer's bank, or sometimes the network, verifies that the customer's account has sufficient funds to pay. The network then contacts the merchant's computer and authorizes the purchase. The network also contacts the two banks, which debit the customer's account and credit the merchant's account. The banks typically do not credit the merchant's account with the entire amount of the transaction: a percentage referred to as the discount is charged by the banks and other intermediaries. Later, usually at the end of the day, the two banks use a different computer network to make a net settlement of all the transfers between them. These steps go unseen and the transaction is completed within minutes.

CREDIT CARDS

Credit cards are fundamentally different from the other payment methods in that they involve extending credit rather than drawing on an existing store of funds. Banks in conjunction with credit card associations such as Visa and MasterCard, issue general-purpose credit cards. Department stores also issue credit cards to be used for purchases at that particular store. Like electronic fund transfers, payment by credit card is not anonymous.

Since paying with a credit card does not involve a store of funds, deposit insurance and reserve requirements are not directly relevant. The bank that issues the card is liable and thus merchants are paid if the cardholder defaults. If the issuing bank fails, the credit card association guarantees payment to merchants with outstanding transactions and then has a creditor's claim on the failed bank.

STORED VALUE CARDS OR SMART CARDS

The new mechanisms for making electronic payments would simply change the first step in the purchase sequence. As an example, the flow of information and funds is discussed here for a generic stored-value card.

The customer buys a stored-value card, such as a Petro Card, with cash or with a debit or credit card. The purchase of the card sets off a chain of settlement transactions according to how that purchase was made. When the customer pays with a stored-value card, the system transfers electronic notations, or tokens, from the card to the merchant's electronic cash register. The merchant periodically contacts the computer network connected to the bank issuing the stored-value cards and presents the tokens for payment. The network then notifies the customer's bank to pay the appropriate sum to the merchant's bank, and the two banks make a net settlement. The banks keep a percentage of the payment (the discount) as compensation for the services they and the networks have provided.

Use of electronic payments will transform cash payments, which typically involve only one bank and no computer network, into a multiparty transaction. The electronic payment mechanisms will be transferring money from one pool of funds, often a segregated account of a bank or other financial institution, to a second pool of funds, usually a checking account in a different financial institution. The consumer will not see most of the actual transfer of funds, as is the case now with purchases using a debit or credit card.

Box 2: Online Payment Methods

An online payment system is needed for compensation for information, goods and services provided through the Internet – such as access to copyrighted materials, database searches or consumption of system resources – or as a convenient form of payment for external goods and services – such as merchandise and services provided outside the Internet. It helps to automate sales activities, extend the potential number of customers and may reduce the amount of paperwork. Given below is a description of online payment methods:

Secure (or Non-secure) Presentation: The customer provides credit card information over a secure (or even clear) transportation means.

Customer Registration: Based on a credit card the customer gets a password or digital signature (hides the credit card information from the merchant, but still clears through the credit card).

Credit-debit Instruments: Similar to customer registration but only one bill per month either through credit card or debit check.

Electronic Currency: This method has potential for anonymity but requires tamper resistant hardware.

Server Scrip: The customer gets a kind of a coupon from an agent that can be spend only with one particular merchant. This reduces the risk of double spending and allows off-line transactions.

Direct Transfer: The customer initiates the transfer of funds to the account of the merchant. This method provides no anonymity.

Collection Agent: The merchant refers the customer to a third party who collects payment using one of the methods mentioned above.

Of all the methods, (non-) secure presentation is the only model that has a large customer base today. All other methods require a special hardware and/or software that most potential customers do not have.

Online Payment Systems

- **Secure Socket Layer (SSL):** Client submits credit card information using encryption based on public keys.
- **CyberCash:** Customer registers credit card with CyberCash and selects a signature key. Requires special software on the client, but hides credit card information from merchant.
- **Secure Electronic Transaction (SET):** The customer obtains a signature key from the card issuer. This method requires special software running on the client to encrypt and sign credit card information.

- **Open Market:** Provides multi-mechanism collection services for web browsers.
- **Mondex:** Provides smart-card based electronic currency.
- **Electronic Check:** Provides a PC card-based credit-debit payment instrument that can be sent across the Internet, but clears through the existing banking network.
- **USC/ISI's NetCheque:** Implements an on-line "checking-account" against which payments are authorized.
- **USC/ISI's NetCash:** Users purchase currency from the currency server using NetCheque. With multiple currency servers, the NetCheque system is used to clear cross-server payments.
- **CMU's NetBill:** Provides a payment instrument analogous to a credit card slip authenticated by Kerberos. Goods are delivered to the customer encrypted; NetBill sends the key to decrypt the goods.

Risks and Security

From the customer's perspective:

- Stolen payment credentials and passwords,
- Dishonest merchants or financial service providers,
- Disputes over quality of services or goods.

From merchant's perspective:

- Forged or copied payment instruments,
- Insufficient funds in customers account, especially with off-line payment systems,
- Dishonest or slow financial service providers.

From the financial service provider's perspective:

- Stolen customer or service credentials,
- Forged or copied payment instruments,
- Customers not paying (applies only to credit models), the risk may be shifted in one direction or the other by using a credit or debit model and by special agreements.

Source: ICFAI Research Center.

Electronic Funds Transfer (EFT) System

No payment systems could boast of excellence unless funds are transferred online. In India, we have the banks maintaining current accounts at the various locations of the Reserve Bank of India. Managing funds flows at these current accounts and providing for transfers from one location to another is yet another activity that could be put over the INFINET. The Reserve bank has introduced Centralised Funds Management System (CFMS) comprising the Centralised Funds Enquiry System (CFES) and the Centralised Funds Management System (CFMS). This paves the way for banks to manage their funds with the RBI in a much more efficient manner and also provide the Treasury/Funds departments of banks with latest information on their balances with the various Deposit Account Department offices of the RBI.

The Reserve Bank of India as part of the initiatives aimed at quick movement of funds in a paperless mode had introduced the Electronic Funds Transfer System (EFT) in the year 1996. Currently, the scheme is available for transfer of funds across 8,500 branches of banks at 15 centers where Reserve Bank of India manages the Clearing House (Ahmedabad, Bangalore, Bhubaneshwar, Chandigarh, Chennai, Guwahati, Hyderabad, Jaipur, Kanpur, Kolkata, Mumbai, Nagpur, New Delhi, Patna and Thiruvananthapuram). The facility is available for transfer of funds for individual transaction upto Rs.2 crore per transaction with effect from 1st October, 2001.

The safest and fastest way to transfer money from your account to another individual in another city regardless of which bank the payee uses is EFT. All the transferor needs is payee's account number. For a flat fee of Rs.25 a maximum of Rs.1,00,000 can be transferred. The bank has discretionary powers to raise the limit for select customers. Or a customer can break up the transactions in to multiples of up to Rs.1,00,000. The money sent is credited overnight and can be withdrawn by the receiver the day after transfer.

The facility can be availed of even if the branch from where you are sending the amount is not fully computerized. The details of the transfer have to be sent to the RBI, which in turn notifies the receiving bank to credit the individual with the mentioned amount.

The Reserve Bank of India is considering a proposal to utilize State Bank of India's clearinghouses to increase the reach of Electronic Fund Transfer (EFT) facility in the country. Almost every district in the country is enabled with the facility of electronic fund transfer with the tie-up of SBI and the central bank.

The EFT package, a software package developed by RBI, can run on even a Windows platform. It was developed in 1996 and is becoming increasingly popular. Over 50 banks have implemented it. For faster processing of transactions and minimizing paper based processing, the RBI gives the software free of charge to banks. EFT enables fund transfer from any branch of any bank, which is a member of the EFT system to any branch of any bank within 24 hours. This includes both inter-city, intra-city and also interbank and intra-bank.

EFT was first tested between Chennai and Mumbai. The year 1997 saw the EFT facility expanded to all metros and in 2002 over to 15 centers in a phased manner. With a maximum amount permitted at Rs.2 crore EFT is primarily aimed at retail transactions.

The establishment of a Real-Time Gross Settlement (RTGS) System for the country would be a natural extension of the above. RBI has done considerable amount of concrete work for the setting up of a RTGS system in the country.

Special Electronic Funds Transfer of Interbank Funds

The SEFT Scheme was introduced by the Reserve Bank of India, in conjunction with banks from April 1, 2003, to provide a safe, secure and same-day electronic transfer of funds across the country.

The Special Electronic Fund Transfer (SEFT) Scheme will have settlement-taking place at Mumbai for interbank funds transfers. The scheme has been made available in over 2,500 bank branches in 500 cities. SEFT facilitates timely settlement of pay-in and pay-out under the proposed T + 2 based rolling settlement in securities at stock exchanges.

The objectives of the RBI SEFT System are:

- To establish an Electronic Funds Transfer System to facilitate an efficient, secure, economical, reliable and expeditious system of funds transfer and clearing in the banking sector throughout India, and
- To relieve the stress on the existing paper based funds transfer and clearing system.

COVERAGE

Initially, the System would cover branches of banks as indicated by the Reserve Bank of India. It is essential that only networked branches of banks are part of the systems to facilitate quick transfer of SEFT messages. Banks' own networks could be used for inter-branch communication. The salient features of the Scheme are:

- The Scheme is designed to provide for same day interbank transfer of funds between accounts maintained in any of the participating branches under the Scheme.
- The Scheme covers branches of banks that are networked so that SEFT messages could be transmitted electronically and quickly.

- Interbank settlement under the SEFT Scheme will be done at Mumbai with the processing being done at the National Clearing Cell, Reserve Bank of India, Nariman Point, Mumbai.
- There will be three SEFT settlement cycles on weekdays (at 12:00 noon, 2:00 p.m. and 4:00 p.m.) and two settlements on Saturday (at 12:00 noon and 2:00 p.m.).
- Credit in respect of inward SEFT requests would be given to the beneficiary's account latest before the next settlement cycle.
- Any credits that cannot be afforded to the beneficiary's account would be returned during the next settlement cycle failing which the credits would be assumed to have been effected.
- The settlement cycles under the SEFT Scheme will be distinct from the existing EFT Scheme, which will continue to operate even after the introduction of the SEFT System.
- The SEFT would cover around 500 cities - with the number of branches exceeding 2500.

The Scheme would facilitate timely settlement of pay-in and pay-out under the proposed T + 2 based rolling settlement in securities at the Stock Exchanges.

Box 3: Procedural Guidelines for (SEFT) Participating Banks[1]

Procedural guidelines detailed hereunder, pertain to participating banks and institutions and the system of computer and communication network through which funds transfer operation would take place.

Definitions

SEFT Center: Means any office designated by the Nodal Department in each of the centers to which EFT system is extended, for receiving, processing and sending the EFT data file and the debiting and crediting of accounts of the participating banks and institutions for settlement of payment obligations or one or more of these functions. National Clearing Center, Mumbai is being designed as the EFT center.

EFT Data File: Means an electronic data file of a batch of payment orders for funds transfers, processed and consolidated in the manner specified for transmission of consolidated payment orders and communications concerning payment orders from EFT service branch to the EFT center.

SEFT Service Branch: Means an office or branch of a bank or institution in a center designated by that bank or institution to be responsible for processing, sending or receiving EFT data file of that bank or institution in that Center and to all other functions entrusted to an SEFT service branch by or under these Regulations. SEFT Service Branch is referred to as "Sending SEFT Service Branch" when it originates an EFT Data File for Funds Transfer. SEFT Service Branch is referred to as "Receiving SEFT Service Branch" when it receives EFT Data File from SEFT Center.

SEFT System: Means the Special Electronic Funds Transfer System established by these Regulations for carrying out inter bank and intra-bank funds transfers within India, through EFT centers connected by a network, and providing for settlement of payment obligations arising out of such funds transfers, between participating banks or institutions.

See Appendix – I, for SEFT Procedural Guidelines as given by the RBI.

Execution of a Payment Order: In relation to a sending bank it means the transmission or sending of the payment order by it to the EFT Service Branch; in relation to a Service branch it means transmission of the consolidated payment order in the encrypted EFT data file to the SEFT center.

1 See Appendix 1, for SEFT Procedural Guidelines as given by the RBI.

Funds Transfer: Means the series of transactions beginning with the issue of originator's payment order to the sending bank and completed by acceptance of payment order by the beneficiary's bank for the purpose of making payment to the beneficiary of the order.

Nodal Department: Means the Department of Information Technology of Reserve Bank which is responsible for implementation, administration and supervision of the SEFT System.

Security Procedure: Means the set of procedural guidelines for the purpose of:

i. Verifying that a payment order, a communication canceling a payment order or an SEFT Data Fie is authorised by the person from whom it purports to be authorised; and

ii. For detecting error in the transmission or the content of a payment order, a communication or an EFT Data File.

Sending Bank: Means the branch of a bank, maintaining an account of and to which payment order is issued by the originator. When the originator is a participating institution, reference to the sending bank shall be construed as referring to the SEFT center.

Settlement Account: Means an account maintained by a participating bank or institution for the purpose of settlement of payment obligations under SEFT Systems.

Valid Reasons of Non-payment: These are the reasons listed as under due to which the beneficiary bank fails to make payment to the beneficiary. Some illustrative reasons are:

i. Beneficiary not having an account with the beneficiary bank.

ii. Account Number or account name indicated in the payment order not matching with the number or name as recorded at the beneficiary bank.

iii. Dislocation of work due to circumstances beyond the control of the beneficiary bank such as earth quake, fire etc., at the place where the beneficiary's account details are maintained etc.

Admission Necessary for Participation: No persons shall be entitled to effect a funds transfer in the SEFT System, unless the sending bank and the beneficiary bank is admitted for participation in the SEFT System. To be eligible to apply for admission, an applicant must-

i. Be a bank.

ii. Have attained and continue to comply with capital adequacy norms, if any, applicable to it.

iii. Be willing and able to comply with the technical operational requirements of SEFT System.

iv. Be approved by the Reserve Bank as eligible to maintain a settlement account with it.

Provided that, having regard to the pattern of ownership and such other relevant factors, all or any of the above conditions may be relaxed or dispensed with, if so decided by the Reserve Bank of India.

Procedure for Admission: Any bank or institution eligible to be admitted in the SEFT System may submit to the Nodal Department, duly authenticated application, containing full particulars in the form specified at Appendix I (Form: SFT-IA) (to RBI Guidelines). Every application shall be accompanied by an undertaking in the specified form to abide by the Procedural Guidelines in the event of admission.

Source: ICFAI Research Center.

THE ELECTRONIC CLEARING SERVICE (ECS)

INFINET, explained in detail later in this chapter, is a high-tech communication facility established by RBI to take Indian Banking to the new millennium. There can be no better measure of success of the INFINET than the facility for quick funds transfer. Over the last few years, the Reserve Bank of India has, developed many new products for the benefit of banks, which are all aimed at ultimately improving customer service and systemic efficiency. One of this - the Electronic Clearing Service (ECS) - is aimed at effecting electronically, repetitive credits or debits for a large population of customers spread across a large number of branches of many banks.

ECS (Credit Clearing)

This is a new method of payment whereby the institutions having to make a large number of payments (such as interest/dividend) can directly deposit the amount into the bank accounts of the share-holders/depositors/investors without having to issue paper instruments.

Bulk and repetitive payments like interest/dividend are mostly paper based involving printing of warrants (in costly MICR format). They are dispatched by post (most often by Regd. post) and reconciled thereof after payment by the agency banks. The difficulties are:

- For printing, dispatch and reconciliation it requires expensive administrative machinery.
- Bunching of a large number of instruments in clearing results in operational bottlenecks and pressures on the cheque processing system.
- Chances of loss of instruments in transit and their fraudulent encashment.
- The customer has also to keep track of the receipt/non-receipt of the instrument and make efforts to deposit the instrument at the bank on receipt of the same.
- Banks find processing of such a large volume of instruments not only error prone and monotonous, but also a strain on the cheque clearing system.

THE PROCESS OF ECS (CREDIT CLEARING)

- **Step-1:** The corporate body institution (called "User"), which has to make payments to a large number of customers/investors, would prepare the payment data on a magnetic media (i.e., tape or floppy) and submit the same to its banker (Sponsor Bank).
- **Step-2:** The Sponsor Bank would present the payment data to the local Bankers' Clearing House (managed by Reserve Bank of India at 15 centers and by State Bank of India or Associate banks at other centers) authorising the Manager of the Clearing House to debit the Sponsor Bank's account and credit the accounts (Destination Bank) of the banks where the beneficiaries of the transactions maintain their accounts.
- **Step-3:** On receiving this authorization, the Clearing House will process the data and work out an interbank funds settlement.
- **Step-4:** The Clearing House will furnish to the service branches of the destination banks branch-wise credit reports indicating the beneficiary details such as the names of the branches where the accounts are maintained, the names of the beneficiaries, account type, account numbers and the respective amounts.
- **Step-5:** The service branches will in turn pass on the advice to the concerned branches of their bank, which will credit the beneficiaries' accounts on the appointed date.

BENEFITS TO A CORPORATE BODY/INSTITUTION

- Savings in administrative cost presently being incurred for printing of paper instruments in MICR format and dispatching them by Registered Post.
- Loss of instruments in transit or fraudulent encashment thereof totally eliminated.
- Reconciliation of transactions is made automatic. By the time the ECS cycle is completed, the user institution gets an electronic data file from its bank with the date of payment and banker's confirmation thereon.
- Cash management becomes easier as arrangement for funds is required to be made only on the specified date.
- Ensuring better customer/investor service.
- Paying the way the best companies in the world pay to their share holders/ investors, customers.

Benefits to the Beneficiary Customer

- Payment on the due date.
- Effortless receipt – No need for visiting the bank for depositing the dividend/interest warrant.
- In case of loss of instrument in transit or fraudulent encashment thereof, consequent correspondence with the company is totally eliminated.

ECS (Debit Clearing)

The Reserve Bank of India has introduced the Electronic Clearing Service (Debit) scheme to provide a faster method of effecting periodic and repetitive payments by 'direct debit' to customers' accounts (duly authorized) thereby minimising paper transactions and increasing customer satisfaction. Electronic Clearing Service (Debit) envisages "a large number of debits and one credit" in the case of collection of electricity bills, telephone bills, loan installments, insurance premia, Club fees, etc., by the Utility Service Providers.

As per the existing system for collection of electricity bills and telephone bills, the customers/subscribers are required to go to the collection centers/designated banks and stand in long queues for payment of bills/dues. There would not be any cash transaction or payment through cheques in the new system. There is an overall limit of Rs.5,00,000 per transaction. Levy of service charges by both sponsoring bank and destination bank is now left entirely to the discretion of respective banks. A sum of Re.0.50 only is collected by NCC, RBI towards Clearing House charges. Utility service providers like MTNL, Telephone/Mobile companies, Telecom Departments, State Electricity Boards, Banks (for collection of credit cards dues) LIC, Housing Finance Companies, Intermediaries and Clubs etc., are making use of ECS (Debit) Clearing system.

THE PROCESS OF ECS (DEBIT CLEARING)

- Utility Companies, banks/institutions receiving periodic/repetitive payments towards electricity bills/telephone bills/loan installments/insurance premia initially collect mandates from their customers/subscribers for collection of amounts due from them by direct debit to their accounts with banks. The mandate provides details such as the name, account number, name of bank/branch etc., duly certified by the bank concerned.
- Based on the details furnished in the mandates, the user company prepares transaction data on electronic media and submits the encrypted data to the local Clearing House, through its Sponsor bank.
- After due validation of the data, the local clearinghouse processes the same and arrives at the interbank settlement as also generates bank-wise/branch-wise reports (hard copies).

- NCC debits the destination banks' accounts with clearing house and simultaneously affords a consolidated credit to the sponsor bank's account and furnishes the bank-wise and branch-wise reports to the service branches of destination banks.
- Service branches forward the branch-wise reports to the respective branches for debiting the accounts of customers with the indicated amounts.

BENEFITS UNDER ECS (DEBIT CLEARING)

- Better cash management by the companies and faster collection of bills.
- Eliminates the need for the customers to go to the collection centers/banks and stand in long queues for payment.
- Automatic debiting to the accounts once the mandates are given by the customers, to that effect cuts down the procedural delay.

Management Information Systems

Yet another area of interest is the Management Information Systems (MIS). Using Information Technology for MIS is ideal and helpful in decision-making. Also INFINET helps to provide the banks the facility to transmit information on currency chests, which would ensure flow of notes and coins as required. INFINET would also provide communication tools for carrying MIS-based data of banks and financial institutions – both for their own internal usage such as periodical statements, data etc., as also for sharing across members critical data such as credit information of customers at the national level, intercity linking of ATMs, facilities for transmission of data for data warehousing purposes, data mining etc. The dissemination of information from the Central Bank to the other members - in the form of circulars, guidelines and the like could also be through the INFINET.

ELECTRONIC DATA INTERCHANGE (EDI)

Electronic Data Interchange (EDI) involves the exchange of structured business documents, such as orders and invoices, directly between computers. Financial EDI extends this process to the payment and settlement process performed by banks. At present EDI is principally used for inter-company communication, removing the need for paper-based transmission of orders and remittance information. Although EDI standards were developed in the early 1980s, actual implementation has been very modest to date. Low take-up rates to date have been explained in terms of high start-up costs, lack of familiarity, as well as overall low take-up rates, which frequently require businesses to maintain dual paper-based and electronic remittance systems in parallel.

The Ministry of Commerce, Government of India has identified 114 centers as major export/import intensive centers in the country. The Ministry desired that, at all these centers, the bank branches should be fully computerised, inter-connected and networked and there should be interbank connectivity so that on-line banking facility could be made available to the exporter-importer customers.

The Department of Commerce in the Ministry of Commerce & Industry, Government of India is the nodal agency for overseeing implementation of Electronic Commerce (EC)/Electronic Data Interchange (EDI) in the various organisations in the country. Banks are one of the agencies entrusted with the responsibility for implementing EC/EDI. The Indian Banks' Association is coordinating the implementation of the EC/EDI in the various banks as per the directives of the Ministry of Commerce & Industry. Currently, 11 Public Sector Banks at 28 locations in the various airports/seaports are implementing the Banks-Customs EDI Project.

Computerization of Payment Systems

The Payment and Settlement System is an essential part of the financial system of a vibrant economy. Consolidation, Development and Integration of the financial infrastructure and reforms in the payment and settlement systems of the country that address the twin issues of safety and efficiency have been engaging the attention of the Central Bankers and Financial Institutions the world over. Payment and Settlement Systems are no longer the backwaters of either the banks or the Central Banks.

The Reserve Bank has taken up the mission critical approach to the establishment of an integrated payment and settlement system in the country. A number of initiatives have either already been implemented or are in an advanced stage on the drawing board. The Systemically Important Payment System (SIPS) has been identified and classified and various measures have been initiated to facilitate real time or near real time large value interbank funds transfer in secured environment.

The Reserve Bank of India has adopted a holistic approach - in which Information Technology is an integral component - encompassing the following:

i. Design and development of a modern, robust, efficient, secure and integrated payment and settlement system;

ii. Risks in payment and settlement systems;

iii. Legal framework;

iv. Impact of payment systems on monetary policy;

v. Concerns relating to oversight of the payment systems; and,

vi. Role and responsibility of different constituents of the payment and settlement systems.

In the design and development of integrated modern payment and settlement systems, the Reserve Bank of India as the Central Bank played a pivotal role, associating at the same time the banking and financial industry in this exercise. A three-pronged approach has been adopted to usher in and establish a modern, robust payment and settlements system consistent with international best practices. The strategy revolves primarily around three major themes:

- Consolidation of the existing Payment Systems;
- Development of Payment Systems; and
- Integration of the Payments and Settlement Systems.

The consolidation of the existing payment systems revolves around strengthening Computerized Cheque clearing, expanding the reach of Electronic Clearing Service – Debit and Credit and Electronic Funds Transfer – by providing for systems with the latest levels of technology.

Integration of the various payment products with the systems of individual banks using the facilities offered by computerization and networking is the current thrust area. Integration requires a high degree of standardization within a bank and seamless interfaces across banks. This would have to be done by standardization of systems whenever the new systems are acquired and old systems are replaced. Development of corporate intranets by banks, and interconnecting the local branches and connecting the computerized branches with the main branches in a city, with the controlling offices, central treasury departments and head offices, making extensive use of INFINET for intra-bank inter city connectivity fall under another focus area.

The RBI's Recent Initiatives include:

- The RBI had embarked on technology based solutions for the improvement of the payment and settlement system infrastructure. Recognizing the importance of payments and settlement systems in the economy of the country, it has introduced of new payment products – such as the Computerized settlement of clearing transactions, use of Magnetic Ink Character Recognition Technology and Image for cheque clearing, operationalization of BANKNET - a leased line terrestrial network, the computerization of Government Accounts and accounting of Currency Chest transactions.
- The new payment products introduced over the last few years included the two-way inter-city cheque collection at the four metros, one-way inter-city cheque collection by clearing houses managed by the Reserve Bank of India and a few clearing houses managed by the State Bank of India, Electronic Clearing Service (Debit and Credit), Delivery versus Payment (DvP) for Government Securities transactions and Electronic Funds Transfer.
- The PDO/NDS/SSS project, comprising inter alia the Negotiated Dealing System (NDS) is an initiative, which provides for an electronic platform for facilitating trading in Government Securities and Money Market Instruments. The System has been operational for over a year now and the manner in which it has been used is laudable. The Securities Settlement System (SSS) will, in the near future, provide on-line depository services for the Government Securities.
- Established at the behest of the Reserve Bank, the Clearing Corporation of India Ltd., (CCIL) has established itself as a Central Counterparty and is presently extending guaranteed settlement for trades done in the Government Securities Market and the Forex market. The number of products launched by CCIL in its short duration of existence speaks volumes of both the CCIL and the financial sector. The forex trading platform, offered by CCIL, for taking care of the settlement of interbank rupee-US dollar deals, provides for a deep, liquid and transparent forex trading facility. This will help in improving market efficiency and integrity.
- Special EFT has been introduced to facilitate funds settlement on T + 0 basis thrice a day. This facility is available from 2500 bank branches located in 500 centers.
- The Centralized Funds Management System is one such initiative, which provides for a Centralized Funds Enquiry System to the treasury branches of the banks in the first phase and the Centralized Funds Transfer System in the second phase, allowing the banks to do an optimal deployment of funds. Most clients have already been actively using the funds enquiry module of CFMS as a platform to have a bird's eye view of their account balances at various Reserve Bank locations. Very shortly, they will be in a position to use this platform to do a near real time transfer of funds between their accounts in pursuance of their day-to-day funds management exercise.

FINANCIAL NETWORKS IN INDIA

A secure dedicated communication backbone has already been developed the RBI – INFINET – for the banking and financial sector. It invites participation by all categories of banks and financial institutions which would benefit out of the usage of this Closed User Group network - such as for the organizations dealing in

Government Securities or those which maintain accounts or perform business with the Reserve Bank of India. The network would be expanded to be a combination of satellite and terrestrial modes of communication and action initiated for inter-connectivity of this network to the network of banks (with adequate security controls in place) to facilitate 'Straight Through Processing' keeping in tune with the advances in technology.

Utilisation of the network by the banking industry through the development of intra-nets; intra-city connectivity to VSATs and development of bank level gateways – The objective of the INFINET would be to provide inter-city and interbank connectivity while banks' own corporate networks could provide inter-branch and intra-city connectivity.

Implementation of the Generic Architecture Model for inter-connectivity of branches within banks – following the 'tree' (for older banks with a tiered management control structure) or the 'star' topology (for the newer banks with a flat management control/reporting structure).

Integration of the message transfer facilities within the country with that of Society for Worldwide Interbank Financial Telecommunication (SWIFT) for 'Straight Through Processing' by inter-connectivity between SWIFT and INFINET.

Internet banking – as a delivery channel for banking services. Using the benefits of the cost-effective medium of Internet, many services or products of banks could be provided in a secure environment where the authenticity of the constituent and the integrity of the message are ensured.

Standardization of technology for all these projects – from hardware, operating systems, system software, application software and messaging middleware. While these would be applicable for all common interbank applications, the software applications at banks could provide for these requirements on the basis of the standards.

Providing for a Common Minimum Requirement Level (CMRL) in terms of hardware and networking requirements of the participants by the payment and settlement systems.

Connecting INFINET and Internet in a secured manner so that some of the services could be extended to the public through Internet as the delivery channel. This could also be for settlement of e-commerce transactions – for the funds leg to be settled using the INFINET with one bank functioning as the settlement bank. Constituents of banks could communicate to the banks through the Internet or through the medium of other private networks; the interface with the INFINET would be based on achievement of minimum safety and security requirements in all such cases.

SWADHAN, the Shared Payment Network Service

The foremost among the electronic payment gateways available in the banking segment is ATM (Automated Teller Machine). It is a computerized device that enables bank customers to withdraw cash outside banking hours. ATMs also accept cash and cheques, provide statements and effect transfers. Operated by cash cards and a Personal Identification Number (PIN), they are placed on outside walls of banks. Of late, the deployment locations of ATMs include hospitals, showrooms, shopping malls and airports.

In India, HSBC set the trend and set-up the first ATM machine in 1987. Since then, they have become a common sight in many of our metros. With more than 800,000 machines worldwide, ATMs have made hard cash just seconds away all through the day at every corner of the globe. ATMs allow one to do a number of banking functions – such as withdrawing cash from one's account, making balance inquiries and transferring money from one account to another – using a plastic, magnetic-strip card and personal identification number issued by the financial institution.

Foreseeing the escalating demand and need for ubiquitous ATMs in the country, The Indian Bank Association promoted SWADHAN in the year 1997 for its member banks to share their ATMs with other participating banks. The drive was to reduce the huge investment required to install ATMs in different locations

SWADHAN, India's FIRST Shared Payment Network Service is unsurpassed in offering countrywide access to the banking operations at more than 1000 ATMs in and around 64 cities. It has 55 member banks in the network, which include nationalized, private and foreign banks. SWADHAN provides convenient banking, 24 hours a day and 7 days a week through the Automated Teller Machines to the participating bank's customers across the country. With SWADHAN, the bank customers are never far away from an ATM.

The member bank's customer can withdraw money anytime from any of the ATM irrespective of the bank with which the customer has an account. It offers services beyond cash withdrawals, like utility bill payment, fund transfer and deposits. SWADHAN widens the scope of ATM usage in the country in a cost effective manner. A member bank of SWADHAN can increase its geographical presence without deploying ATMs in all the locations; instead it can share and use ATMs of other banks, thereby saving a substantial amount. Likewise, the customer of the bank is highly benefited by having a nation-wide access to the card, without holding multiple accounts in different banks.

The largest and only Shared Payment Network System (SPNS) in India, SWADHAN is posting a very impressive growth rate since its inception. In 1997, at the start of the network, the number of ATMs in the SWADHAN Network was only around 24, whereas today it has grown close to 1,000 ATMs i.e., about 25% increase. Each day new ATMs and banks are added to the network.

Being the leading light in Shared Payment Network System for debit cards in India, it has auspicious plans to provide connectivity to the international payment networks, such as master card and visa in a very formidable way. It is poised to enable the existing system for e-payments thereby helping the banks excel in an e-powered service.

With Swadhan it was hoped that customers would be able to benefit from an ATM pool that solved the problems of single-ATM outlet banks and its attendant problems of limited access, distance and time.

The Main Features of Swadhan are:

- No exchange fee charged to change an old ATM card for a Swadhan card.
- Rs.3,000 fixed as the ceiling on withdrawal.
- Exception made for select customers who can withdraw up to Rs.10,000. Still, this is lower than the average withdrawal of Rs.15,000 by regular ATMs.

- IBA gives banks the discretion to decide a higher maximum amount for withdrawal.
- Transactions conducted through any of the member banks appear on a bank statement, which is given only by your own bank.
- All transactions conducted in any of the member banks appear on the bank statement, but only your own bank will provide this information.

However, no overdraft facility is available on Swadhan cards.

Let's take a look at how the system works.

A switch routes all information and transactions among member institutions. It transmits the information and/or data to the card-issuing bank or its processor, which approves or declines the transaction request and notifies the switch. The card-issuing bank's decision is then routed by the switch to the processor of the ATM, which completes the transaction. At the end of each day, accounts among members are settled and account balances are transmitted to each member institution.

Box 5: BankNet

Recognizing the pressing need to harness information technology for intra-bank and interbank communication the RBI set-up BANKNET in 1985. The design and implementation of BANKNET was entrusted to M/s. CMC Ltd.

The BANKNET infrastructure uses RBInet, which is a communication software to provide message and file transfer between branches of banks and across banks.

Commissioned in 1991, BANKNET is a packet switched X.25 based network with nodes at Mumbai, Delhi, Chennai and Calcutta, and a switching center at Nagpur with a mesh topology. In addition, Bangalore and Hyderabad connected to Chennai through remote PADs. IBM 4381 mainframes at the 4 NCCs, connected to nodal Packet Switch Exchanges (PSEs) through Front-End processors using NCP/NPSI (Network Control Program/Network Packet Switching Interface), provide messaging facility. BANKNET uses a store-and-collect transmission logic, provided by the Message Transfer Utility (MTU), in the systems.

User banks access BANKNET through leased lines at the respective local centers using asynchronous ports on PADs and PC/UNIX machines with COMET (Computerised Message Transfer and File Transfer) software, developed in 'C'. The Message Transfer Utility enables 400 users to login at a time at each IBM node.

COMET has facilities for message creation, deletion, editing, ascertaining status of messages, listing and receiving acknowledgement etc. It also permits free format messages of 8 lines of 48 characters each.

Various message format templates, similar to SWIFT formats are available in COMET. Message formats for funds transfer applications such as TT issue, TT Purchase and TT Confirmation, Bank transfer on own account, Bank transfer in favor of a third party, etc. are available. Similarly several message formats for critical data transmission activities such as reporting weekly statement of accounts, daily and monthly balances of Government accounts, agency transactions in Government accounts, transfer responding advices, foreign currency rates, advice of cheques for collection, balance queries, inter-city advices etc. too are available.

Source: ICFAI Research Center.

Indian Financial Network (INFINET)

The INFINET is the communication backbone of the Indian Banking and Financial sector. All Banks – Public Sector, Private Sector, Foreign, Cooperative etc., and premier Financial Institutions in the country are eligible to become members of the INFINET.

The INFINET is a Closed User Group (CUG) Network and uses a blend of communication technologies such as VSATs and Terrestrial Leased Lines. The network consists of over 700 VSATs located in 127 cities of the country and utilizes one full transponder on INSAT 3B. The Hub of the VSAT network is situated at the IDRBT, and is manned round the clock. Various interbank and intrabank applications ranging from Simple Messaging, MIS, EFT, ECS, Electronic Debit, Online Processing and Trading in Government Securities, Centralised Funds querying for Banks and Financial Institutions, Anywhere/Anytime Banking, and Inter-Branch Reconciliation are being implemented using the INFINET.

Box 6: INFINET (Indian Financial Network)

The INFINET is primarily a TCP/IP based network. A detailed IP addressing scheme has been devised by IDRBT for all CUG members, which has to be strictly followed by all CUG members while interacting via the INFINET communication backbone. Every CUG member has to sign a Memorandum of Understanding with IDRBT to avail the services.

Remote VSAT: The Remote VSATs consist of two kinds of equipment. The first type works on TDMA/TDM technology and it is typically used for data transfers. The other works on DAMA technology, which is generally used for data transfers of approximately 64 kbps and more, voice and video.

Mail Messaging System: IDRBT has set-up a Mail Messaging System (MMS) on the INFINET for enabling basic communication between the users. MMS consists of high availability e-mail servers, which perform Clustering, Load Balancing, Certification, Domain Name Services etc. A unique set-up has also been made so that users of these e-mails can also send and receive mails from the Internet. Using this messaging backbone, banks can implement highly effective and productive workflow applications on the INFINET.

MMS is being used to provide a unique Corporate e-mail facility to the banks. Banks can now have a simple short e-mail address for their executives and officers across the country, like designation@bankname.co.in or username@bankname.co.in. The advantage of this facility is that it enables users to have a single, permanent e-mail address, which can be used, on their Corporate Intranet as well as on the Internet. The designation based official email addresses provide instant access to the new incumbent or ever-changing incumbents and the username based demi-official e-mail address provides instant access to the particular person, wherever he goes, on multiple transfers and so on, without the need for changing the e-mail address.

Banks can also implement security for their messaging and e-mail applications, using digital signatures and certification to take care of authentication, authorization, confidentiality, non-repudiation etc.

Structured Financial Messaging Solution: IDRBT is implementing the Structured Financial Messaging Solution (SFMS) to provide a reliable platform for domestic financial messaging. Its key features include:

- Modularised web-enabled software enabling financial messaging within and between the participating banks.
- Template builder to support flexible definition of messages similar to SWIFT like user-to-user and systems messages.

- Flexible architecture that facilitates centralized or distributed deployment.
- Directory services for maintenance of IFSC directory, network configuration.
- Secured messaging and routing based on store and forward principles governed by push technology.
- Messages can be clubbed and exchanged as a batch of files.
- Smart card based user access.
- Messages will be secured via standard encryption and authentication services conforming to ISO/SWIFT standards.
- Complete auditing, logging, time-stamping and warehousing of messages.
- Periodic computation of charges and billing of the services offered to the participating banks.
- Multi-tiered solution covering INFINET Hub, Bank Gateways and Bank sites.

Security: The INFINET is the most secure platform that technology can provide for this purpose. Here are its salient features:

- INFINET being a CUG, provides a high level of security against intruders. Outsiders cannot enter or penetrate the network.
- In the case of VSAT Network, the IP Addresses for IDUs at the remote VSAT locations are allotted and maintained by the Hub and cannot be changed by the endusers. This takes care of the network integrity and security.
- In the space segment, the data transmission, even in broadcast mode, is encrypted using proprietary standards and the packets cannot be opened at any VSAT location except the one specified as the destination VSAT.
- In the case of Leased Line Network (LLN) IPSEC 56 will be used to provide state-of-the-art encryption and security.
- Apart from the above layers of network security, there will be a host of in-built security mechanisms in each application that is deployed on the INFINET – like password, access control, encryption, digital signatures and certification and in some applications there will be smart card and/or bio-metric authentication as well.
- Application level Security at par with international standards is provided through Symmetric Key and Public Key Cryptography and IDRBT will act as the Certification Authority for the Banking and Financial Sector.

Application: INFINET can be used for both intra and interbank applications. Banks can develop and port intra-bank applications on their own. Interbank applications are being developed together by the Reserve Bank of India, IDRBT and member banks. Applications such as Real Time Gross Settlement, Central Funds Management System, Security Settlement System, Electronic Clearing System and Electronic Funds Transfer, being developed by the RBI will be ported on the INFINET and in a true sense, the INFINET will become the backbone for the National Payment Systems. These applications will use the SFMS platform.

Some of the applications, which the CUG members are using on the network are Any Branch Banking (Multi Branch Banking), Fast Collection of Cheques, Cash Management Products, ATM Network, Interbank reconciliation, Corporate E-mails etc.

Source: ICFAI Research Center.

REAL-TIME GROSS SETTLEMENT SYSTEM (RTGS)

The Real-Time Gross Settlement System is the key critical element and provides the missing link in the process of the setting up of the Integrated Payment and Settlement System in the country. The world over, the Real-Time Gross Settlement System is now, the preferred mode of the settlement of large value interbank payments, with more and more countries moving towards it. In the SAARC region, India is now being joined by Sri Lanka, which has also decided to move over to RTGS.

As a settlement process, RTGS minimises settlement risks by settling individual payments in real time in the books of account, held at the Central Bank. Under RTGS, the practically instant settlement ensures fast, secure, final and irrevocable settlement of payment transactions. The Real Time Gross Settlement system is designed to provide large value funds transfer and settlement in an on-line real time environment to the banking industry, with settlement on a gross basis. An integral component of the Real Time Gross Settlement system will be the Delivery versus Payment module for trading and settlement in Government Securities transactions. The system would have links with other netting systems like Clearing, Automated Clearing House transactions comprising Electronic Clearing Service, Retail Electronic Funds Transfer, all Plastic Money and Smart Card transactions and Electronic Funds Transfer at Point of Sale (EFTPOS).

A large value funds transfer system, whereby financial intermediaries can settle interbank transfers for their own account as well as for their customers, the RTGS system effects final settlement of interbank funds transfers on a continuous, transaction-by-transaction basis throughout the processing day.

The system went 'live' on March 26 with State Bank of India, HDFC Bank, Standard Chartered Bank, and Saraswat Co-operative bank. The Reserve Bank of India expects 120 scheduled commercial banks and primary dealers to become part of the RTGS. ICICI Bank, IndusInd Bank, BNP Paribas, Bank of Baroda, Bank of India, Canara Bank, Central Bank of India, Corporation Bank and Union Bank of India are likely to join shortly.

The statistics of transactions for the month of March 2004, shows that in the interbank market transactions involving 45,000 instruments and aggregating Rs.1,79,000 crore were settled. High value instruments (3,17,000) settlement aggregated Rs.2,74,000 crore. However, settlement of MICR instruments (145 lakh) accounted for only Rs.54,000 crore. RTGS will eliminate settlement risk in the case of interbank and high value transactions.

Banks could use balances maintained under the Cash Reserve Ratio (CRR) instead of the Intra-Day Liquidity (IDL) to be supplied by the central bank for meeting any eventuality arising out of the RTGS. The RBI has fixed the IDL limit for banks to three times their Net Owned Fund (NOF). The IDL will be charged at Rs.25 per transaction entered into by the bank on the RTGS platform. The marketable securities and treasury bills will have to be placed as collateral with a margin of five percent. However, the apex bank will also impose severe penalties if the IDL is not paid back at the end of the day.

Box 7: Centralized Funds Management System
The Reserve Bank started the process of putting in place a Centralized Funds Management System for the benefit of the banks in the year 1998-99. The Centralized Funds Management System envisages connecting all the Deposit Accounts Department of the Reserve Bank located at seventeen Regional offices with the Apex Level Server located in Mumbai. The Centralized Funds Management System (CFMS) facilitates funds and treasury managers of commercial banks, which are ready with the infrastructure for obtaining the data in a networked environment to query and obtain the consolidated and account-wise, center-wise position of their balances with all the Deposit Accounts Departments of the RBI, installed at the various RBI locations. The system envisages periodical updation of Current Account balances in the Apex Level Server whenever a transaction is put through at the local or remote Deposit Accounts Department. The Bank Level Server will be able to query the Apex Level Server to check on its "global" or overall funds position. Eventually, funds transfer facility will be made available. While the first phase of the system covering the Centralized Funds Enquiry System (CFES) has been made available to the users, the second phase comprising the Centralized Funds Transfer System (CFTS) would be made available by the middle of 2003. So far, 54 banks have implemented the system at their treasuries/funds management branches

Source: ICFAI Research Center.

Payment Messaging Systems and SWIFT

Electronic payment systems for large payments have developed as the demands for international settlement of currency and securities transactions have increased. Society for Worldwide Interbank Financial Telecommunication known as SWIFT, currently dominates the field of interbank messaging but is increasingly facing competition from other networks. SWIFT was set-up in 1973 and is based in Brussels. Its member banks, a consortium of more than 2,200 banks own it. SWIFT provides electronic payment services to around 4,300 financial institutions worldwide and presently processes around 500 million payment messages a year. Shares in SWIFT are based on the volume of message traffic. SWIFT has been criticized for relying on hub and spoke communications technology, which was originally conceived in the 1970s. Although the SWIFT system enjoys worldwide acceptance it is dependent on the same heritage of correspondent banks, which form the basis for all low value cross-border transfers.

Box 8: SWIFT
SWIFT provides messaging services to banks, broker/dealers and investment managers, as well as to market infrastructures in payments, treasury, securities and trade. These services help customers reduce costs, improve automation and manage risk. SWIFT is a cooperative society under Belgian law and is owned and controlled by its members. It has a Board of up to 25 Directors who are responsible for overseeing and governing the company. The Board oversees the Executive, a team of full-time employees headed by a Chief Executive Officer. The Executive is responsible for the preparation, integrity and objectivity of the consolidated financial statements and other information presented in the Annual Report. The basic objectives of SWIFT are to: i. Work in partnership with its members to provide low-cost, competitive financial processing and communication services of the highest security and reliability. ii. Contribute significantly to the commercial success of its members through greater automation of the end-to-end financial transaction process, based on its leading expertise in message processing and financial standards setting.

iii. Capitalize on its position as an international open forum for the world's financial institutions to address industry-level threats, issues and opportunities.
iv. Employ and recruit the best people, invest in the most beneficial resources, and become a leading global organization respected for its professionalism, effectiveness, vision and management.

SWIFT was started with the mission of creating a shared worldwide data processing and communications link and a common language for international financial transactions. SWIFT makes sure that the financial institutions that will use the messages are heavily involved in the development process to ensure effectiveness and practicality.

Emphasis on Security and Reliability

Rules defining responsibility and liability are written, operational practices put in place. Fundamental principles behind SWIFT are established at an early stage. Because SWIFT's shareholders represent a broad international base, best practices from several countries have influenced the Company's governance. The Board has seven committees with delegated decision powers: Audit and Finance, Banking and Payments, Compensation, 'E', Securities, Standards, Technology and Production.

SWIFT is committed to an open and constructive dialogue with oversight authorities. Oversight on SWIFT is based on a special arrangement by the central banks of the G10 countries, represented by the Committee on Payment and Settlement Systems (CPSS). Under this arrangement, the National Bank of Belgium, the central bank of the country in which SWIFT's headquarters are located, acts as lead overseer of SWIFT, supported by the central banks of the G10. The issues discussed can include all topics related to systemic risk, security and availability. Topics that overseers discussed in 2001 with SWIFT include the implementation of SAS 70, Trust Act, the security audit findings, and selected management processes relating to security and availability. Discussions on the latter also touched upon security and availability of SWIFT services in the light of the network subcontracting arrangement with Global Crossing.

Over the years, SWIFT has grown into a worldwide service-provider. As of end 2001 it had 7457 live users in 196 countries and handled 1,534,000,000 messages the same year.

Operations of SWIFT in India

SWIFT User Group is formed in India with the Chairman IBA as the Chairperson and the Chief General Manager-in-Charge, Department of Information Technology, Reserve Bank of India as the Alternate Chairperson. Currently there are 92 institutions comprising banks, brokers and dealers, central depositories and clearing organizations, who are the user members of SWIFT in India:

- Members 48
- Sub-Members 36
- Broker(s) and Dealer(s) 1
- Central Depositories and Clearing 1
- Non-Shareholding Banks 5
- Representative Office(s) 1
- Total 92.

Single-window access to and for the global financial industry is the ambition underpinning SWIFTNet. In 2001, SWIFTNet messaging services saw the first fully live implementations by domestic market infrastructures: the Bundesbank's RTGSPlus system and the Bank of England's Enquiry Link. SWIFT was scheduled for open migration to the SWIFTNet services from July 2002. The SWIFT users in India would also need to migrate from the current X.25 connectivity protocol to the Next Generation IP (Internet Protocol) based SWIFTNet services. To facilitate a smooth migration, the SWIFT users in India will have to get adequate training and education on the technical aspects and

other related information on the SWIFTNet services. SWIFT is planning to conduct a series of workshop/seminars for the SWIFT users in India for disseminating the technical, operational and other related information on the SWIFTNet services.

Recognition of Indian Financial System Code (IFSC) by SWIFT

The banks in India are being connected through the INFINET for Interbank and Intra-bank transactions electronically. The INFINET is a VSAT based closed user group network for the exclusive use of the banking and financial sector. There is a closed user group comprising members who have joined the INFINET for initiating Interbank and Intra-bank electronic transactions through the network. The closed user group has decided that to facilitate ease of usage and create inter-operability between the various members of its network standard message formats be designed and developed for most of the common applications on the network. Accordingly, a Committee of Bankers in India deliberated on the issue and decided that an eleven digit coding pattern be introduced for identifying the bank/financial institution and their branches when transactions are initiated through the network. This system of eleven digit coding pattern called "Indian Financial System Code (IFSC)" shall also be included in all SWIFT international messages to facilitate routing of the messages direct to the beneficiary branch in India and thus putting in place "Straight Through Processing (STP)" on a large scale. For achieving the above, the Committee of Bankers has recommended that a routing symbol "//IN", may be introduced which will uniquely identify messages meant for India and the beneficiary branch in India and the same be registered with SWIFT as India's National Routing Code.

The SWIFT has considered the above recommendations of the Committee of Bankers and the National Clearing Code (Routing Code) for India ("//IN") has now been incorporated by SWIFT in its routing system.

Source: ICFAI Research Center.

PUBLIC KEY INFRASTRUCTURE (PKI)

Authentication in transactions is offered by Public Key Infrastructure (PKI). Usually stored in a secure media such as a smart card or an i-key or even a floppy disk, PKI provides an electronic identity to a person through the issuance of a digital certificate and a private cryptographic key. The person could make use of the identity to digitally sign documents or transactions. Objectives of PKI Software are:

- To reduce risk of fraud in electronic fund transfers and other treasury activities.
- To use a low-cost public network infrastructure and eliminate the need for dedicated leased lines or VPNs.
- To facilitate real-time cash management with strategic banking partners.
- To ensure that only specific users can access and execute high value transactions.
- To integrate the software easily with legacy systems.

The Need for PKI

Lack of trust and security over existing and evolving infrastructures is the greatest obstacle to e-business in the financial service sector. For e-business transactions to flourish all parties involved in transactions and communications must be able to confirm the unique and irrefutable digital identity of each participant before relying on that information to make a commercial transaction.

But when it comes to making high value transactions, such as setting up an online cash management system, even for the so-called online banking systems or procuring supplies through the Internet, there is too much at stake in simply trusting someone just because he gave the correct PIN or the correct username and password. Developing systems that are able to provide firm authentication of

customers, suppliers and other parties have therefore become a major challenge. The solution to provide trustworthy identities such as Public Key Infrastructure (PKI) systems have emerged.

In the case of online banking for users, banks need to have a proper system for authentication of the user. The user is still identified using the typical username/id verification process that is vulnerable to hacking, even though banks have a secure network system for encrypted data transfer. So, implementation of PKI makes sure that the party performing a transaction over the Internet is who he claims to be. Later he cannot deny that he has not done a particular transaction, if he had used his digital certificate.

Benefits and the Use of PKI

One can prove to a third party or the court that a particular piece of electronic document is authentic and can be traced to the person who has digitally signed the document or transaction, through the use of PKI and digital signature. This works because the cryptography and mathematics underlying a PKI system ensure that digitally signed documents cannot be forged. The digital certificate can be thought of as the electronic equivalent of the identification card. Thus, the authority which issues the digital certificates (known as Certificate Authority) must be highly trusted and secure.

Technology, legal framework and standards are other issues related to PKI besides security. The technology for PKI has been around for more than a decade and is relatively mature and a number of countries have introduced legislation to recognize the validity of a digital signature.

A standard for business transactions has been enabled by the introduction of IT Laws by many countries. Forums like Asia Pacific PKI Forum allow inter-operability to its digital certifying authority licensees with their counterparts in the member countries of that region. Their customers will create an extensive global system of known and trusted businesses, as financial institutions sign on to these policies and business practices. A trading partner can authenticate any other party with assurance once certified by a Certification Authority. Even if a trading partner is from another part of the world, the fact that he is a certified member (through the trust relationship with his bank) makes trading viable and reduces the risk of transacting in the global system. By virtue of commonly accepted standards, trading partners will know that:

- Their transactions are legally binding;
- In the event of a dispute or a potential fraud situation they have recourse; and
- They can place legal and practical trust on the electronic identity issued by any Certification Authority.

How PKI Works

Before examining the components of a PKI it is necessary to understand some of the basics of encryption, digital certificates and digital signatures.

ENCRYPTION OVERVIEW

"Encryption" is the term used to describe the process of taking legible data, and scrambling it into a form that is non-intelligible to anyone who doesn't know how to unscramble (or "decrypt") it again.

Encryption processes usually involve a method for encrypting the data and one or more "keys". The keys are usually a very long number, and are used during the encryption or decryption process.

In most cases, the method (or "algorithm") that is used by an application to encrypt data is common knowledge and the key that is used is kept private.

There are two main types of encryption – "symmetric encryption" (the same encryption key is used for encryption and decryption), and "asymmetric encryption" (different keys are used for encryption and decryption).

Asymmetric encryption algorithms use two keys – a "public key" and a "private key". The algorithm usually involves a mathematical step that is very easy to do one way, but very difficult to do in reverse.

DISTINCT FEATURES OF ALGORITHM

Algorithm is designed such that:

- Anything that is encrypted using the public key can be decrypted with the private key.
- Anything that is encrypted with the private key can be decrypted with the public key.
- The keys are generated in such a way that it is not possible to determine one key if you know the other.

This method of encrypting data using a widely publicized public key and separate private key is also called "Public Key Cryptography" and is the type of encryption that is utilized by digital certificates.

DIGITAL CERTIFICATES

A "certificate" means, "a document testifying to the truth of something". A digital certificate is an electronic "certificate" that contains information about a user and is used (among other things) to verify who the user is. Digital certificates make use of Public Key Cryptography. The public key is stored as part of the digital certificate. The private key is kept on the user's computer, or in some hardware such as smart cards, i-keys etc. Digital certificates are based on the IETF X.509 series of documents. The main uses of digital certificates are:

- Proving the identity of the sender of a transaction, non-repudiation and checking the integrity of transmitted data (via the use of digital signatures).
- Encryption.
- Single sign-on (the digital certificate can be used as an authorization key to connect to computer systems.)

If digital certificates are to be used for security and identification purposes, all of the following conditions must be met:

- Every certificate must be unique.
- The owner of a certificate has been fully identified. All digital certificates are signed by the Certificate Authority (CA) that issues it. In issuing a certificate, the CA is basically saying that it has identified the user, and the user really is who he claims to be. To be able to trust a digital certificate, the CA needs to have fully identified the customer before issuing the certificate (or be satisfied that some other entity has adequately performed such identification).
- The owner of the certificate can alone use a private key. As with all authentication schemes, the onus is on the user to keep the private key private. Usually a password, a smart card or biometric device is used to lock the private key and prevent others from using it.

Digital Signatures

A digital signature is used to verify the integrity of a block of data. Digital signatures are also used to verify the identity of the person who sent the transmission.

A digital signature is created as follows:

- A "digest" of the data is created. The digest is a short length of binary information and is based entirely on the contents of the data. A hashing algorithm such as MD4 or SHA is used to create the "hash" or digest. Hashing algorithms are designed such that changing just one character in the message would result in a different hashed value.

- The hash is then encrypted using the private key of the person who is sending the message.
- The encrypted digest is known as a "digital signature" and is attached to the message when it is sent.

When the message is received:

- A hash of the message is again created, using the same hashing algorithm.
- The sender's public key is used to decrypt the digital signature, and this is compared to the digest of the message that has been generated by the receiver's software.
- If both hashes are the same, then the data in the message has not been altered during transmission.

Given that only the owner of the digital certificate can create the digital signature (because he is the only person who has access to the private key), attaching a digital signature to a transmission also proves the identity of the person who sent it.

PUBLIC KEY INFRASTRUCTURE

A Public Key Infrastructure (PKI) is made up of various software-based services and encryption technologies that are used to facilitate trusted and encrypted transactions over an insecure network.

In most practical implementations of a Public Key Infrastructure digital certificates are used. The PKI for an organization typically includes the following components:

- Digital certificates – one for each user and server.
- A Certificate Authority (CA) responsible for issuing certificates.
- One or more Registration Authorities (RA) that are responsible for identifying users during the digital certificate registration process.
- A Directory service – used to store information about users, including their public key.
- The Directory service is usually based on the LDAP or X.500 protocols.
- Software that is capable of using digital certificates.

Certificate Authority (CA)

A third party that is responsible for issuing digital certificates to users is a Certificate Authority (CA). Each digital certificate is digitally signed by the CA's private key that the CA issues.

This is to ensure that the digital certificate has not been tampered with.

Each CA has its own procedure for identifying users. The procedure is usually listed in the CA's Certificate Practice Statement (CPS). Identification procedures range from little or no identification, to a user having to provide 100 points worth of ID before being issued with a digital certificate.

Ideally, a CA is trusted, and always follows the advertised Certificate Practice Statement.

Typically, browser software (for example, Niyamas Tyootelery) gives users the option of marking a given CA as trusted or not trusted. A Certificate Authority also runs and maintains the server that contains the certificate database, and a list of any certificates that have been revoked, and publishes public keys and the revocation list into a publicly accessible directory service. The CA is also responsible for making sure that the server itself is physically secure, and that the CA's private key is not compromised. Certificate Authorities are usually arranged in a "chain" where any given CA has its root key signed by the next CA up the chain. The CA at the root or the top of the chain signs its own root key. If a given

CA is trusted by a user's software, every subordinate CA below it in the CA chain is automatically trusted since the trusted CA has vouched for the trustworthiness of all Certificate Authorities below it.

Registration Authority (RA)

They need to be identified according to the procedures of the Certificate Authority that is issuing the certificate before a user can be issued with a digital certificate. A separate Registration Authority (RA) often handles this registration process.

A Registration Authority is responsible for identifying users and notifying the Certificate Authority that the user is allowed to be issued with a digital certificate. The RA does not sign or issue digital certificates directly.

SUMMARY

- Traditional payment methods include cash, cheques, electronic fund transfers, and credit cards. Unlike other methods of payment, which involve changing notations in the ledgers of financial institutions, payment by cash is an immediate physical transfer of funds. Each method of payment differs in terms of the regulations covering it and the degree of privacy, anonymity, and protection it conveys to consumers. Internet and World Wide Web came to be extensively used in banking transactions in a number of ways. This has provided immense benefit to the customers, and ensured total accuracy of transactions. The concept providing services to the customers for 24 hours per day and 7 days per week (any time, any where banking) became possible without the customer visiting the bank, but remaining at his own place before his desktop.
- Electronic Fund Transfers (EFTs) are ways of transferring notational money from one account to another or converting notational money into cash. Such transfers are initiated through an electronic terminal, telephone, computer, or magnetic tape to authorize a financial institution to debit or credit a consumer's deposit account. The Electronic Clearing Service (ECS) is aimed at effecting electronically, repetitive credits or debits for a large population of customers spread across a large number of branches of many banks. Electronic Data Interchange (EDI) involves the exchange of structured business documents, such as orders and invoices, directly between computers. Financial EDI extends this process to the payment and settlement process performed by banks. At present, EDI is principally used for inter-company communication, removing the need for paper-based transmission of orders and remittance information.
- The RBI has developed the secure dedicated communication backbone – INFINET – for the banking and financial sector. This provides the network for participation by all categories of banks and financial institutions which would benefit out of the usage of this Closed User Group network – such as for the organizations dealing in Government Securities or those which maintain accounts or perform business with the Reserve Bank of India. SWADHAN, India's first Shared Payment Network Service is unsurpassed in offering countrywide access to the banking operations at more than 1000 ATMs in and around 64 cities.
- Recognizing the pressing need to harness information technology for intra-bank and interbank communication the RBI set-up BANKNET in 1985. The INFINET is the communication backbone of the Indian Banking and Financial sector. All Banks, Public Sector, Private Sector, Foreign, Cooperative etc., and premier Financial Institutions in the country are eligible to become members of the INFINET. It is primarily a TCP/IP based network and can be used for both intra and interbank applications. The Real Time Gross Settlement System is the key critical element and provides the missing link in the process of setting up the Integrated Payment and Settlement

System in the country. The Real-Time Gross Settlement System is now, the world over, the preferred mode of settlement of large value interbank payments, with more and more countries moving towards it.

- SWIFT, which stands for the Society for Worldwide Interbank Financial Telecommunication, currently dominates the field of interbank messaging but is increasingly facing competition from other networks. SWIFT provides messaging services to banks, broker/dealers and investment managers, as well as to market infrastructures in payments, treasury, securities and trade. These services help customers reduce costs, improve automation and manage risk. SWIFT was started with the mission of creating a shared worldwide data processing and communications link and a common language for international financial transactions. Public Key Infrastructure (PKI) systems offer authentication in transactions. PKI provides an electronic identity to a person through the issuance of a digital certificate and a private cryptographic key, usually stored in a secure media such as a smart card or an i-key or even a floppy disk. The person could make use of the identity to digitally sign documents or transactions.
- A “certificate” means: “A document testifying to the truth of something”. A digital certificate is an electronic “certificate” that contains information about a user and is used (among other things) to verify whom the user is. Digital certificates make use of Public Key Cryptography. A digital signature is used to verify the integrity of a block of data. Digital signatures are also used to verify the identity of the person who sent the transmission.

Appendix I

Special Electronic Funds Transfer System: Procedural Guidelines

Section - 1 : Introduction

Section - 2 : Definitions

Section - 3 : Participants

Section - 4 : Seft-Process Flow

Section - 5 : Inter-Bank Settlement

Section - 6 : Rights and Obligations.

SECTION – I: INTRODUCTION

Introduction

1.1 Reserve Bank of India has introduced a system called "The Reserve Bank of India Special Electronic Funds Transfer System" which may be referred to as "SEFT System" or "System" and shall include the set of procedural guidelines detailed hereunder, for participating banks and institutions with the required system of computer and communication network through which funds transfer operation would take place.

Objects

1.2 The objects of the SEFT System are:

To establish an Electronic Funds Transfer System to facilitate an efficient, secure, economical, reliable and expeditious system of funds transfer and clearing in the banking sector throughout India, and

To relieve the stress on the existing paper based funds transfer and clearing system.

Coverage

1.3 Initially, the System would cover branches of banks as indicated by Reserve Bank of India. To facilitate quick transfer of SEFT messages, it is essential that only networked branches of banks are part of the systems. Banks' own networks could be used for inter-branch communication.

SECTION - 2: DEFINITIONS

2.1 In these Procedural Guidelines, unless the context otherwise requires:

a. "Acceptance" means execution of payment order.

b. "Bank" means a banking company as defined in Section 5 of the Banking Regulation Act, 1949, and includes the State Bank of India, constituted by the State Bank of India Act, 1955, a Subsidiary Bank constituted under the State Bank of India (Subsidiary-Banks) Act, 1959, a Corresponding new bank constituted under the Banking Companies (Acquisition and Transfer of Under-taking) Act, 1980, a co-operative bank, as defined in Section 56 of part V of the Banking Regulation Act, 1949 and such other banks as may be specified from time to time.

c. "Beneficiary" means the person designated as such, and to whose account payment is directed to be made in a payment order.

d. "Beneficiary bank" means the branch of the bank identified in a payment order in which the account of the beneficiary is to be credited.

e. "SEFT" means Special Electronic Funds Transfer.

f. "SEFT Center" means any office designated by the Nodal Department in each of the centers to which SEFT system is extended, for receiving, processing and sending the SEFT data file and the debiting and crediting of accounts of the participating banks and institutions for settlement of payment obligations or one or more of these functions. National Clearing Cell, Nariman Point, Mumbai is being designed as the SEFT center for purposes of the SEFT System.

g. "SEFT Data File" means an electronic data file of a batch of payment orders for funds transfers, processed and consolidated in the manner specified for transmission of consolidated payment orders and communications concerning payment orders from SEFT service brach to the SEFT center.

h. "SEFT Service Branch" means an office or branch of a bank in a center designated by that bank to be responsible for processing, sending or receiving SEFT data file of that bank in that Center and to do all other functions entrusted to an SEFT service branch by or under these Regulations. SEFT Service Branch is referred to as "Sending SEFT Service Branch" when it originates an SEFT Data File for Funds Transfer. SEFT Service Branch is referred to as "Receiving SEFT Service Branch" when it receives SEFT Data File from SEFT Center.

i. "SEFT System" means the Special Electronic Funds Transfer System established by these Regulations for carrying out inter bank and intra-bank funds transfers within India, and providing for settlement of payment obligations arising out of such funds transfers, between participating banks.

j. "Execution" of a payment order in relation to a sending bank means the transmission or sending of the payment order by it to the SEFT Service Branch; in relation to a Service branch it means transmission of the consolidated payment order in the encrypted SEFT data file to the SEFT center.

k. "Funds Transfer" means the series of transactions beginning with the issue of originator's payment order to the sending bank and completed by acceptance of payment order by the beneficiary's bank for the purpose of making payment to the beneficiary of the order.

l. "Nodal Department" means the Department of Information Technology of Reserve Bank which is responsible for implementation, administration and supervision of the SEFT System.

m. "Notified" means communicated electronically or in writing.

n. "Originator" means the person who issues a payment order to the sending bank.

o. "Participating Bank" means a bank admitted for participating into the SEFT System pursuant to Paragraph 3.1 of these Guidelines and who's Letter of Admission has not been cancelled.

p. "Payment Order" means an unconditional instruction issued by an originator in writing or transmitted electronically to a sending bank to effect a funds transfer for a certain sum of money expressed in Indian rupees, to the designated account of a designated beneficiary by debiting correspondingly an account of the originator.

q. "Public Sector Bank" means State Bank of India, constituted by the State Bank of India Act, 1955, subsidiary Banks constituted under the State Bank of India (Subsidiary Banks Act, 1959, the banks constituted under Section 3 of the Banking Companies (Acquisition an Transfer of undertaking) Act, 1970 and the Banks constituted under Section 3 of the Banking Companies (Acquisition and Transfer of Undertaking) Act, 1980.

r. "Reserve Bank" means the Reserve Bank of India established under the Reserve Bank of India Act, 1934 (2 of 1934).

s. "Security Procedure" means the set of procedural guidelines at Paragraphs under the Sections of these Guidelines for the purpose of:

   i. Verifying that a payment order, a communication authorising a payment order or an SEFT Data Fie is authorised by the person from whom it purports to be authorised; and

   ii. For detecting error in the transmission or the content of a payment order, a communication or an SEFT Data File.

t. "Sending bank" means the branch of a bank, maintaining an account of and to which payment order is issued by the originator. When the originator is a participating institution, reference to sending bank shall be construed as referring to the SEFT center.

u. "Settlement Account" means an account maintained by a participating bank or institution for the purpose of settlement of payment obligations under SEFT Systems

v. "Valid Reasons of Non-payment" are the reasons listed as under due to which beneficiary bank fails to or cannot make payment to the beneficiary. Some illustrative reasons are:

   a. Beneficiary not having an account with the beneficiary bank.

   b. Account Number or account name indicated in the payment order not matching with the number or name as recorded at the beneficiary bank.

   c. Dislocation of work due to circumstances beyond the control of the beneficiary bank such as earth quake, fire etc. at the place where the beneficiary's account details are maintained etc.

   d. Any other valid reason preventing passage of the credit – such as a court order restraining operations on the beneficiary's account.

SECTION - 3: PARTICIPANTS

Admission Necessary for Participation

3.1 No persons shall be entitled to effect a funds transfer in the SEFT System, unless the sending bank and the beneficiary bank is admitted for participation in the SEFT System. Whenever the branch of a bank appears in the list of branches offering SEFT Services on the designated website that branch is deemed to have been admitted under SEFT System.

Eligibility for Admission as a Participant

3.2 To be eligible to apply for admission, an applicant must:

i. Be a bank.

ii. Have attained and continues to comply with capital adequacy norms, if any, applicable to it.

iii. Is willing and able to comply with the technical and operational requirements of SEFT System,

iv. Be approved by the Reserve Bank as eligible to maintain a settlement account with it.

Provided that, having regard to the pattern of ownership and such other relevant factors, all or any of the above conditions may be relaxed or dispensed with, if so decided by the Reserve Bank of India.

All members of the Electronic Funds Transfer (SEFT) system are automatically eligible to become members of the SEFT.

Procedure for Admission

3.3 Any bank or institution eligible to be admitted in the SEFT System may submit to the Nodal Department, duly authenticated application, containing full particulars in the form specified at Annexure-I (Form: SFT-IA). Every application shall be accompanied by an undertaking in the specified form to abide by the Procedural Guidelines in the event of admission.

3.4 The Nodal Department shall issue Letter of Admission as specified in Annexure-II (Form: SFT-IB) to every bank admitted into the SEFT System.

3.5 A directory of participating banks shall be prepared from time to time and would be available through the RBI website.

Suspension

3.6 If a participating bank has defaulted in meeting its settlement obligations or paying any charges or fees or complying with any procedural guidelines or for any reasons specified at paragraph 3.15, the Letter of Admission issued to it is liable to be kept under suspension for such period as may be specified in the order of suspension.

3.7 Every order of suspension shall be notified immediately to all the participating banks and institutions including a bank or institution against which the order of suspension is passed.

3.8 An order of suspension may be reviewed and may be revoked at any time by the Governor, Reserve Bank of India upon representation received from the concerned bank or on his own. Every revocation shall be notified immediately to all participating banks.

3.9 A participating bank shall not, while any order of suspension is in force against it, be entitled to send or receive any SEFT data file 2`or otherwise to effect any funds transfer in the SEFT System.

Provided that a suspension shall not affect the obligations of the suspended bank or institution, whether incurred before or after the suspension.

Withdrawal

3.10 Any participating bank or institution may, by giving a notice of one month, withdraw from the SEFT System.

3.11 No notice under this Regulation shall be effective unless it is given in writing and before the expiry of one month from the date of receipt of notice by the Nodal Department.

3.12 Notwithstanding its withdrawal, a bank shall discharge all its payment obligations arising out of fund transfers attributable to it, whether effected before or after the withdrawal became effective.

3.13 The withdrawal of any participating bank shall be notified to all the participating banks.

Cancellation of Letter of Admission

3.14 A Letter of admission issued to any bank may be cancelled by the Reserve Bank on its being satisfied that such bank has -

i. Defaulted in complying with any Regulations or procedural guidelines issued thereunder from time to time.

ii. Been placed under an order of moratorium or an order prohibiting acceptance of fresh deposits or an order of winding up or in respect of which a provisional liquidator has been appointed.

iii. Stopped or suspended payment of its debts.

iv. Failed to get the order of suspension passed against it under Regulation 8 revoked within a period of three months from the date of order of suspension.

v. Has conducted its transactions in the SEFT System in a manner prejudicial to the interest, integrity or efficiency of the System.

3.15 No order of cancellation shall be passed without first giving an opportunity of hearing to the bank concerned.

3.16 Every order of cancellation shall be notified to the respective bank and also to all other participating banks in the SEFT System.

3.17 Notwithstanding the order of cancellation of Letter of Admission passed against it, such bank discharge all its payment obligations arising out of the funds transfers effected in the SEFT System.

SECTION - 4: SEFT - PROCESS FLOW

4.1 The parties to a funds transfer under this SEFT System are the sending bank, the sending service branch, the SEFT center, the receiving service branch and the beneficiary branch.

Request for SEFT by Bank Customer

4.2 A bank customer (i.e. Sender or originator) willing to avail of the remittance facilities offered by a sending bank shall submit an “SEFT Application Form” authorising the sending bank to debit the sender’s account and transfer funds to the beneficiary specified in the SEFT Application Form.

4.3 Each participating bank/institution may design the format of “SEFT Application Form”. A model SEFT Application form is given at Annexure-III (Form: SFT-2A).

4.4 The sender's request for transfer of funds shall contain no condition other than date on which funds transfer process should be initiated.

4.5 The relationship between the customer (i.e. sender) and the sending bank will be governed by an Agreement to be executed between them. The Agreement shall govern every payment order issued by the customer during the period of validity of the Agreement. A Model Customer Agreement is given at Annexure-IV (Form-2B).

4.6 The value of each SEFT transactions shall be for whole rupees only. This stipulation may be clearly indicated on the SEFT Application Form.

4.7 The upper limit for individual SEFT transaction or payment order shall be fixed by the Nodal Department. Till further advice from the Nodal Department, the limit shall be Rs.2,00,00,000/- (Rupees two crores only) per transaction.

4.8 A transaction within the SEFT system will be said to have been initiated when the sending bank accepts a payment order issued by the sender by issuing a "receipt" indicating the date of initiating funds transfer operation and the likely date on which the beneficiary bank may make payment to the beneficiary.

4.9 If in a single payment instruction, the sender directs payments to several beneficiaries, each payment direction shall be treated as a separate payment order.

4.10 A bank branch may reject a customer's request for funds transfer when, in the opinion of the remitting branch,

i. The customer has not placed funds at the disposal of the sending bank; or funds placed is not adequate to cover the sum to be remitted and the service charge; or

ii. The beneficiary details given in the SEFT Application form are not adequate to identify beneficiary by the beneficiary bank. The essential elements of beneficiary's identification are:

Beneficiary's Name	:	]
Center Name	:	]
Beneficiary Bank Name	:	] could be codified also
Beneficiary Branch Name	:	]
Beneficiary's Account Type	:	
Beneficiary's Account No.	:	

4.11 The sending bank shall prominently display at its premises the cutoff time schedules up to which shall receive the SEFT Application Forms from its customers for different settlements.

SEFT Scroll

4.12 The sending bank would consolidate the applications received till the cutoff time and forward the SEFT data to the service branch via the network.

Data Entry at Sending SEFT Service Branch

4.13 The sending SEFT service branch shall prepare SEFT Data File by using the software package supplied by the Nodal Department (NCC, Nariman Point, Mumbai). Control procedure should be developed by the sending bank to ensure accuracy in data entry with reference to the data elements furnished in SEFT file. After SEFT Data File is consolidated from various branches, the Service Branch should generate consolidated SEFT file and transmit the same to the SEFT center. There shall be only one service branch per each bank.

National Clearing Cell (NCC) to Function as SEFT Centre

4.14 The National Clearing Cell (NCC), of the RBI at Mumbai will be the data processing "SEFT Center".

Transmission/Submission of SEFT Data File to the SEFT centre

4.15 The remitting service branch shall transmit the SEFT Data File to the SEFT centre by using the communication network designated by Reserve Bank.

4.16 The data files would be transmitted to National Clearing Centre in such a manner that they reach well before the settlement zones to be notified by the Nodal Department. To begin with three settlements would be conducted at 12.00 noon, 2.00 p.m. and 4.00 p.m. on week days and 12 noon and 2,00 p.m. on Saturdays.

Receiving NCC Transmitting NCC Data File to the Beneficiary Banks

4.17 After consolidating all SEFT Data Files received from the participants the NCC shall process the data and generate the settlement of each beneficiary bank which has at least one inward remittance transaction on an NCC Data File.

4.18 NCC Data files generated for the banks will be available in the secure website and each bank needs to download the file immediately after the conclusion of each settlement zone.

Data Validation at Receiving SEFT Service Branch

4.19 On receipt of the NCC Data File, the receiving SEFT service branch shall first validate the file using the validation routine provided in the SEFT package. Apart from the validation with reference to the encryption key exchange with local NCC and checksum total for the entire file, the package would validate the individual records as well.

Payment to Beneficiary by the Beneficiary Bank

4.20 The service branch should transmit the branch wise data immediately on receipt from National Clearing Center to the beneficiary branches.

4.21 The beneficiary branches would make payment to the beneficiaries instantly on the same day by crediting the specified account of the beneficiary or otherwise placing funds at the disposal of the beneficiary.

Revocation of Payment Order

4.22 A payment order issued for execution shall become irrevocable when it is executed by the sending bank. Any revocation, after the payment order is executed by the sending bank shall not be binding on any other party in the SEFT system.

Acknowledgement by the Beneficiary Bank

4.23 No acknowledgements are envisaged under SEFT Scheme. A message, which is not returned unaffected before the next settlement zone is treated to have been completed and credited afforded to the beneficiary's account by the beneficiary branch. It is therefore vital that unaffected credits are re-transmitted back as fresh SEFT transactions at the immediate next settlement itself.

Sender to be Advised in Case of Refund

4.24 If the beneficiary specified in the sender's payment order fails to get payment through the SEFT system for some valid reasons, the sender shall be informed immediately after the sending bank gets the returned SEFT. The sending bank shall also arrange to make payment to the sender by crediting the account of the sender or otherwise placing funds at the disposal of the sender.

Beneficiary Bank to Advise the Beneficiary of the Payment

4.25 After crediting the account of the beneficiary, the beneficiary bank shall advise the beneficiary of the payments made. The Statement of account/Pass Book entry or any online messaging system shall indicate briefly the source of funds as well.

4.26 The sender/originator shall be entitled to claim interest at the Bank Rate from the sending bank for the period of delay in the completion of funds transfer, and/or any other penalty which may be levied/decided by RBI

4.27 In case of holiday at beneficiary branch. They have to effect the credit as on the same day or latest at commencement of business on the next working day.

SECTION - 5: INTER-BANK SETTLEMENT

Inter-bank Funds Settlement at Reserve Bank

5.1 Every participating bank and admitted institution shall open and maintain in the SEFT center, Mumbai, a settlement account for settlement of payment obligations arising under the funds transfer executed under the SEFT system.

SECTION - 6: RIGHTS AND OBLIGATIONS

General Rights and Obligations of Participating Banks or Institutions

6.1 Every participating bank or institution admitted in the SEFT System shall, subject to compliance with the procedural guidelines, be entitled to execute any payment order for Funds Transfer to a beneficiary of the payment order, issued or accepted by it.

6.2 Every participating bank or institution shall maintain the security, integrity and efficiency of the System.

Obligations of Sending Bank

6.3 The sending bank shall not execute a payment order without complying with the security procedure. No payment order shall be accepted for execution in the SEFT System if the beneficiary's bank / branch is not a participating bank or institution.

6.4 The sending bank shall be responsible for the accuracy of the name of the beneficiary, the nature and style of the account and account number of the beneficiary, the name of the beneficiary's bank and the authenticity of every payment order executed by it.

6.5 The sending bank shall bear the liability for loss if any caused to any participant in the SEFT System on account of the acceptance by it of any revocation of a payment order after it has executed it.

6.6 The sending bank shall not be entitled to bind any other participants in the SEFT System with any "special circumstances" attached to a payment order accepted by it.

6.7 The sending bank shall maintain duly authenticated record of all payment orders executed by it for a period for which bank records are required to be preserved under the applicable rules.

6.8 The sending bank shall, upon completion of funds transfer of a payment order, furnish to the originator on request by him, a duly authenticated record of the transaction.

Obligations of the Sending SEFT Service Branch

6.9 The sending SEFT Service Branch shall be responsible for the accuracy of the contents of SEFT data file and the authenticity of the payment orders contained therein as received by the SEFT Center in compliance with the security procedures.

6.10 The sending SEFT Service Branch shall be responsible for settlement of all payment obligations in regard to payment orders executed by it.

6.11 The sending SEFT Service Branch shall be responsible for ensuring execution of the SEFT data file complying with security procedures and time schedule.

6.12 The sending SEFT Service Branch shall ensure, before execution of any SEFT Data File that the balance in its settlement account are adequate to cover its settlement obligation and ensure that the ceiling, if any, specified for it is not exceeded and the requirement of collateral if specified by the Nodal Department is adequate for execution of the SEFT data file originated by it.

6.13 The sending SEFT Service Branch shall generate, dispatch and maintain records of transaction in accordance with procedure specified.

Obligations of SEFT Center

6.14 Receiving SEFT Center shall be responsible for receiving and processing the Data Files complying with the security procedure and time schedule specified for the purpose.

6.15 The SEFT Center shall in compliance with time schedule and security procedure, process and sort out the Data File bank-wise and after crediting the settlement accounts with the corresponding value, transmit the NCC Data Files to the respective receiving SEFT Service Branches.

6.16 The SEFT Center shall generate, dispatch and maintain records of transactions, in accordance with the procedure specified.

Obligations of the Receiving SEFT Service Branch

6.17 Receiving SEFT Service Branch shall be responsible for receiving NCC Data File from the receiving SEFT Center in accordance with procedure specified.

6.18 Receiving SEFT Service Branch shall process the NCC Data File in compliance with the security procedure and sort-out the payment orders into branch wise lots and transmit to the respective branches the payment orders for execution in accordance with the time schedule and in compliance with the security procedure.

6.19 Receiving SEFT Service Branch shall generate, dispatch and maintain records of transaction accordance with the procedure specified.

Rights and Obligation of Beneficiary Bank

6.20 The beneficiary bank shall execute the payment order on the SEFT working day on which the payment order is received by it unless it notices one or more of the following deficiencies.

a. The beneficiary specified in the payment order has no account or the account of the beneficiary maintained by the beneficiary's bank does not tally with the account specified in the payment order.

b. The beneficiary bank is prevented by instructions of the beneficiary not to give or receive any credit to the account.

c. The account designated in the payment order is closed.

6.21 The beneficiary bank may reject a payment order on one or more of the grounds mentioned in Clause (a) above. The beneficiary bank shall notify, in the manner specified, the sending bank of the rejection of the payment order along with the reasons thereof in the next settlement.

Processing Charges

6.22 A charge shall be levied by the SEFT center for SEFT processing. The current rate is Rs.2/- per transaction.

Source: The Annexures are available at httpp:/www.rbi.org.in/sec7/eft-annx.doc

Chapter VIII

Payment and Settlement Systems, RTGS and Clearing House

After reading this chapter, you will be conversant with:

- Emerging New Instruments
- Risk Factors for Payments Systems
- International Standards on Payment Systems
- Role and Concern of Central Bank and Participants
- Payment and Settlement Systems in India
- Real Time Gross Settlement
- Developments in the Payment and Settlement Systems
- Clearing House

Payment systems constitute the means by which interbank transfer of funds takes place across both domestic and international financial systems and markets. A Payment system is a process that comprises a set of instruments for effecting payments. It is built on the strength of an institutional and organizational framework that regulates payments. Within this process, operating procedures are established and communications networks are maintained. The sophistication of the system depends on the level of requirement. A typical modern payment system contains various subsystems, which serve particular needs of customers, both in terms of the volumes of transactions and values of payments. The payment system holds the key in so far as such payment systems take into account factors such as the speed, financial risk, reliability and cost of domestic and international transactions.

Undoubtedly in today's scenario of international business environment that comprises integrated financial markets, rapid economic growth is facilitated by the operation of efficient payments systems. However, at the same time one should be aware of the challenges that are posed in terms of managing the situation that has arisen as a result of the operation of such systems. The startling fact is that the payments system can also transfer 'shocks' at lightning speed. Hence, for promoting and maintaining financial stability, the requirement of the hour is the presence of robust payment systems. During the past few years, globally, there has been a consensus on the need to strengthen payment systems. This can be made possible only by having uniform and internationally accepted standards and practices meant for the design and operation of payment systems.

EMERGING NEW INSTRUMENTS

The patterns under which payment systems are being conducted have been undergoing changes. In a traditional payment system cheques are issued, collected and payment received against the same. However, consequent to the innovations that have been taking place in this area as a result of technologies being used, new instruments of payment systems have merged. We discuss about them in the following paragraphs:

Electronic Payment Media

The new electronic community is trying to replace paper and plastic with electrons, just as medieval bankers replaced gold with paper and modern bankers substituted plastic for paper. Electronic payment systems are not new. Electronic funds transfer for settling large banking and commercial transactions has been in use since the middle of the last century. Online credit and debit card systems are also electronic. However, these transactions are conducted through closed commercial networks, the main obstacle, to wire fraud. Their security is enhanced through encryption – the enigma cipher machine was based on this technology. In contrast, the Internet is an open system making security much more of a problem. The challenge is to develop open systems that are secure, convenient and cost-effective over a range of micro-to-macro transactions. Anonymity would also be a commercial advantage for many types of Internet transactions.

Electronic Money

As with new terms related to the Internet, e-money refers to various items in different contexts. But most people regard the two major forms of e-money as the smart or Stored Value Card (SVC) and network money or so-called cyber money. A smartcard is a physical card with an embedded computer chip or magnetic stripe that stores the owner's value, while network money is stored in pure electronic form as 0s and 1s in computers and can be transferred over telecommunication networks such as the Internet. Moreover, a hybrid of the two forms can be developed and users may further switch between e-money and conventional deposits or even other payment media. A number of e-money schemes have been

developed but most are still in the fledging stage. The proliferation or failure of e-money depends not only on the customer acceptance, but also on the firms, incentives to develop and promote this. Firstly, the issuer of e-money commits to provide specified quantities of goods at any future time, which can be either instantaneous or far into the future. As a special type of debt, e-money can be used as a source of financing, especially an operation. Second, companies may sue the issuing of e-money as a competition strategy. The development of e-money involves strong network effects, just as in computer operating systems, telephone networks and ATM cards, which mean that the more the people using it, the better it is for all the current users in the network. As it gains popularity e-money will become more liquid, transferable, convenient and less risky.

Digital Money

It is one of the most modern payment systems. However, it has made little headway in the payments market. At the moment, almost all Internet transactions are settled using credit and debit cards. These are widely held, convenient and accepted by most retailers. Yet, plastic cards are by no means ideal for a digital world. They were originally designed for making face-to-face transactions in the real world. Despite attempts to tighten security, including the introduction of micro-chip based cards, they remain prone to fraud and moral hazard. These systems involve a lot of paperwork and are costly to operate. They are expensive for merchants and cannot be used efficiently for making small transactions or for person-to-person transfers. Electronic media has clear advantages over card systems in all of these respects. Security is easier to maintain online through encryption and dedicated servers than offline, where operatives handle security information in readable form. Because they eliminate paper billing and other costs, all electronic media are much cheaper than hybrid paper-electronic systems. The processing costs of digital cheques are about cash and cheques, their digital equivalents can also be used in person-to-person transactions.

Smartcards

They have potentially important role to play in reducing the risk of social exclusion from the electronic payments system. They also offer an efficient way of organizing social security payments. Smartcard technology is currently being adopted by many social security systems.

Pseudo-Cash

In the real world, token money is based either upon items like precious metals and stones that have intrinsic or alternative use value, or on objects such as notes and coins that are essentially valueless but generally accepted as media of exchange. To retain its value, the first kind of token must be scarce and the second hard for counterfeiters to reproduce. Digital products such as software, are generally useful and valuable, but can be reproduced by the provider at zero marginal cost. This characteristic immediately rules out a token money of the first kind. It also makes it difficult to devise a digital token that cannot be reproduced by forgery. In view of these obstacles it is not surprising that no one has yet been able to devise a true token money for the Internet – something that circulates without trace. Digital currencies are actually pseudo-cash because they involve an intermediary and are not in continuous and decentralized peer-to-peer circulation like real world notes and coins. They look like decentralized token money and can be used for person-to-person transactions. However, these transactions are in fact intermediated by the service provider. To make the system secure against double spending each digital coin is returned to the provider by the seller and cancelled after being used once. The coin is then re-issued with a different serial number to the seller. These systems are notational and not token money media.

Digital Cheques

Although these facilities have been available for some time, they are as yet little used. This is surely because of the network effect to catch on; they need more people to accept them. Digital cheques have all of the advantages and disadvantages of paper cheques but, being electronic involve only a third of the processing costs. They can be used for peer-to-peer transactions. They are also subject to counterparty risk. This is a major drawback at the moment given the difficulties of assessing creditworthiness and identity in the electronic marketplace. However, digital certificates and signatures have the potential to resolve these security problems effectively. So does real time settlement, which is technically feasible but not deployed in the market.

The Prospects of Digital Money

The future seems fraught with problems and speculations in this area have proved very wide off the mark. Yet it seems clear that in the near-term, credit and debit cards will remain dominant for large domestic transactions. These are convenient for the consumer and carry a subsidy in the form of a zero interest period and bonus points. Another impetus could come from the use of digital cheques to undertake the peer-to-peer transactions, which plastic money systems do not accommodate. This is where the adoption of new encryption systems is critical. These new systems incorporate digital certificates and signatures that tackle the electronic identity problem. Digital certificates are designed to authenticate websites, so that users know that they are genuine and can submit credit card of compromise. Digital signatures are the electronic equivalent of the handwritten signature and unique to the holder. They verify identity and address that can be used to validate digital cheques and other payment instructions. Importantly, the recipient of a digitally signed instruction can ascertain whether it has been tampered with during transmission. Cheap fingerprint or handprint could also provide another form of Internet identification. There has always been an argument that introduction of digital money would reduce the velocity of circulation and pose problems for the monetary authorities. This might make conventional monetary aggregates a much less useful lead indicator. Indeed, if digital money were to be adopted by the formal economy, leaving notes and coins circulation in the informal economy, this could actually make monetary indicators more useful. The case-in-advance effect would make credit balances associated with pre-pay devices such as cards and phones a useful lead indicator for the formal economy. The correlation with GDP as currently measured should improve. At the same time, physical cash could be used to monitor the development of the underworld economy. At the moment the issue of large denomination notes provides an indication, but such holdings may be legitimate, reflecting hoarding and international currency substitution effects.

EFTPOS (ELECTRONIC FUNDS TRANSFER AT POINT OF SALE)

EFTPOS is another important and modern technique in payment mechanisms. It consists of electronic cash registers called tills. These tills are connected to both retailer's and banks' computer through local area network over wide area network. The retailer's computer contains complete information about the stock control database. This database provides tills with complete information about each product. It also keeps track of all the completed transactions. At the checkout, the operator scans the bar code of each item individually. The price of each product is added to the total and printed on the till receipt. The price and description of each product is displayed on the checkout monitor for the operator and the customer to see. The retailer can always make use of the stock control database, which is automatic, to view the stock levels. A minimum re-order level may be set so that the retailer may be alerted to items that fall below this level and a new order can be sent to their supplier. This may help prevent the shop from running out of popular items and maintain customer satisfaction.

Conversely, items that are not selling well can be easily identified by querying the database. The retailer may then decide to put these on special offer. The customer is offered various payment options: cash, credit card or debit card. Payment by debit card results in Electronic Funds Transfer at Point of Sale. The sequence of activities to complete funds transfer is: the shopper's debit card is swiped through the reader attached to the electronic till at the checkout. The bank sort code, account number, card number, expiry number and issue number are read. The shopper's card details, together with the retailer's identification code (Merchant ID) and purchase total are coded and sent to a central electronic funds transfer switch system. The electronic switch system sends a request for card authorization to the bank's computer. An authorization and authorization code are generated if there is enough money in the shopper's account to pay for the goods. A record is created to settle up between the shopper and retailer's banks 2 or 3 days later. Alternatively, the authorization may be rejected because of insufficient funds in the account. The central switch system sends a message with the result to the till at the checkout. If authorization is granted a debit payment slip with an authorization code is printed for the customer to sign. The transaction is then completed and a card voucher with details of the transaction is given to the customer as a record to keep. The transaction will also appear on the shopper's monthly bank statement. The retailer's card voucher has the following details printed on it on completion of the transaction:

- Date and time of transaction
- Merchant ID
- Transaction code
- The card number, expiry date and issuing bank (payment by switch)
- The payment total
- Summary.

EFTPOS provides retailers the means to process sales and payments automatically.

The connectivity between the stock database and sales also allows for automatic stock control.

RISK FACTORS FOR PAYMENTS SYSTEMS

The payments systems operate under different types of risk environment. These are:

i. Credit risk, which arises in the case of a customer who is unable to meet his financial obligations.

ii. Liquidity risk, which arises in the case of a customer who has insufficient funds. Such customers could fail to meet financial obligations specifically at the time of requirement of such funds.

iii. Legal risk that arises out of the existence of poor legal framework or prevalence of legal uncertainties that lead to increase in the severity of credit or liquidity risks.

iv. Operational risk that arises out of operational factors such as technical malfunctions or operational mistakes that lead to increase in the severity of credit or liquidity risks; and

v. Systemic risk that arises out of the inability of a participant to meet the obligations. This can also be in the form of a breakdown or a disruption in the system that leads to a failure on the part of other participants of the financial system to meet their obligations. This also results in increased severity of liquidity and credit risks.

From the above, it can be observed that while there are different types of risks, the basic risks that really stand out and threaten the system are two: Liquidity and Credit risks.

In the above background, there have been various reasons for the establishment and maintenance of payment systems. Such reasons are as follows:

i. An efficient payment system enables a bank to protect and enhance its brand name for the simple reason that the bank in particular and the banking system in general will benefit from such funds, instead of any other financial intermediary.

ii. An efficient payment system enables a bank to strengthen its customer base by virtue of the services rendered.

iii. An efficient payment system enables a bank to reduce its bank's operating costs and also increase income by operating electronic clearing systems.

There is still a need and concern for worldwide uniformity in standards as far as the payments systems are concerned.

Box 1: Banking at ICICI

Anywhere Banking

- Cheques issued payable at par at various ICICI Bank locations.
- Single account to be operated at any ICICI Bank branch for this facility.
- Ideal for small value, large volume payments.

Fund Transfers

- Online transfer of funds between accounts maintained with any branch of ICICI Bank.
- Issue of Bulk Demand Drafts/Pay Orders.
- Capability to issue Bulk Demand Drafts/Pay Orders on various ICICI Bank and correspondent bank locations.
- Capability to accept online requests from the customers.
- Capability to print beneficiary advice and dispatch.
- Remote printing facility.
- Simple process with a low turnaround time and delivery.

Cheque Writing

- Cheques can be issued on behalf of companies.
- Capability of processing large volumes of cheques in a short turnaround time.
- Capability of printing facsimile signatures.
- Capability to print beneficiary advice and dispatch.
- Ideal for bulk payments such as pension payments, gratuity payments.

At Par Payments

- Services can be availed for the 'at par' payment of dividend warrants/interest warrants/refund order/redemption payments/brokerage payments.
- Simplified and streamlined procedures ensuring smooth process flow, online validation of instruments before payment. Regular reconciliation statements provided by the bank.
- Covering over 100 major locations through own network (90% of the payments). Arrangement with correspondent banks thereby covering over 200 locations through instrument based payments.
- ECS credit facility at all available locations.

Source: icicidirect.com

INTERNATIONAL STANDARDS ON PAYMENT SYSTEMS

Core principles for systemically important payment systems are being developed by the Committee on Payment and Settlement Systems (CPSS) of the central banks of the Group of Ten countries. For this purpose, the CPSS constituted a Task Force on Payment System Principles and Practices in May, 1998. It was to consider the principles that should govern the design and operation of payment systems in all countries. The Committee realized that the Payment Systems do indeed have certain faults. In view of the inherent weaknesses, the core principles that have been developed and suggested have indeed factored in such weaknesses and made suggestions for removing them.

Ideally, a payment system should have the following core principles:

i. The system should be built on a clear legal basis. We must consider the fact that today's cross-border transactions in which different currencies are used by different banks world over, must follow practical and enforceable rules and procedures.

ii. Different participants in the system such as the system operators and customers should gain clarity regarding the financial risks arising out of their participation in the system. Thus, they should understand the financial risks in the system and the manner in which the liabilities are met. Further, the public should be made aware of the key rules relating to financial risks.

iii. With regard to the management of credit risks and liquidity risks, the system should put in place well-defined procedures. It should specify the responsibilities of the system operator and the other participants.

iv. It is very important that the system should materialize the final settlement on the day of value itself. Thus, it should be in real time. This is particularly important since the degree of credit and liquidity risks depends upon the gap between time at which payments are accepted for settlement by the payment system and the actual time of the final settlement.

v. The risk in the case of a multilateral netting system is that if one participant is unable to meet settlement obligations, it puts credit and liquidity pressures on the other participants at the time of settlement. Hence, the system should ensure the completion of daily settlements.

vi. The most preferable asset is the balance held in the account with the Central Bank. Since it is preferred that the assets used for settlement should be by way of a claim on the Central Bank, such balance also represents a claim on the Central Bank. Any other assets that are used should have minimal credit risk.

vii. The payment system should have high degree of security and operational reliability. In case of contingencies alternative arrangements should exist for timely completion of daily processing. Effective business procedures and well-trained and competent personnel should be present to maintain and operate the system.

viii. The payment systems should provide good quality of service, be efficient, safe and provide service at least cost.

ix. The system should be fair and open. The objectives should be clear and disclosed to the public. The system should thus contain features of transparency, accountability and effectiveness.

Payment systems operate in a worldwide environment, and the core principles that have been envisaged are applicable to payment systems of different types. Such systems could involve either credit or debit mechanism, operate either electronically or use paper-based instruments. It has to be said that systems that use paper-based debit instruments (e.g. cheques) face difficulties in complying with some of the principles. In such systems there is a need to consider options other than cheques.

The objectives behind the above mentioned core principles are to use them as universal guidelines and encourage the designing and operation of safer and efficient payment systems. It is obvious that for the purpose of settlements in the payment system, the most preferable asset is balance in the account held with the central bank. Any claim on balance in the account held with the Central Bank carries minimal liquidity and credit risk. Alternatively, any other asset proposed to be used for the purpose of settlement should also have minimal liquidity and credit risks.

ROLE AND CONCERN OF CENTRAL BANK AND PARTICIPANTS

In view of the importance of funds held in the account with Central Bank, we take a look at the role and responsibilities of the Central Bank and also of the participants.

i. The Central Bank's role must be clearly defined and the payment system objectives should be disclosed to the public. In particular, in such environment wherein private sector payment systems exist, participants and users of all systems in general should understand the role, responsibilities and objectives of the Central Bank with regard to payment systems.

ii. The manner in which the Central Bank plans to achieve its objectives must be clear. Thus, the Central Bank should have clear objectives. The major policies that will affect the operators and users of systems must also be defined clearly and disclosed. By doing so, the objectives are not only well understood, but support can also be built for such systems.

iii. The Central Bank should ensure that the systems that are operated by it comply with the core principles. The payment system works to build stability of the system based on the core principles.

iv. The Central Bank should ensure the compliance with the core principles by systems, which are not self-operated, but operated by others such as private payment systems. The extent and degree of compliance depends on the country's legal and institutional framework. While in some countries it is based on statute in some other countries it is based on custom and practice.

v. The Central Bank should ensure that it has the necessary expertise and skills to perform its role of overseeing payment systems. Such function has to be performed in such a manner that the private sector systems are not put to any disadvantage and ensure that the combination of public and private sector provision meets the public policy objectives.

vi. In its role of promoting payment system safety and efficiency, the Central Bank of a country should cooperate with central banks in other countries. Cooperation is particularly important for systems that are characterized by cross-border or multi-currency features.

vii. Authorities such as legislatures and finance ministries are also interested in the safe and efficient functioning of payment systems. Hence, for the fulfillment of the public policy goals, a cooperative approach is required.

Apart from the Central Bank and the government authorities, the participants also need to adhere to certain principles. These are:

i. There is a need to enhance the quality of customer service and also to enhance the quality of delivery of the products and services. Therefore, there is a need for extensive use of information technology, which requires huge investments. In this context, we can view the thrust given by the banks to achieve cent percent branch computerization and networking of banks. As a result appropriate legal and security systems should also be put in place.

ii. With advances in technology there is a huge potential to change the methods of advertising, marketing and designing of products. Consequently, the pricing and distribution of financial products and services have to be cost-effective. Thus the new demands are to have a new, dynamic, aggressive and challenging work culture so that the varying objectives of customer relationships, reputation, corporate governance and regulatory prescriptions are achieved.

iii. There has to be an attitudinal change in the mindset of bankers. They should be prepared to provide services through innovative and secure means.

PAYMENT AND SETTLEMENT SYSTEMS IN INDIA

The Reserve Bank has taken up the mission critical approach to the establishment of an integrated payment and settlement system in the country. A number of initiatives have either already been implemented or are in an advanced stage on the drawing board. Identification and classification of the Systemically Important Payment System (SIPS) have been done and various measures have been initiated to facilitate real time or near real time large value interbank funds transfer in secured environment.

Recent initiatives taken in this regard are discussed below:

i. The PDO/NDS/SSS project, comprising *inter alia* the Negotiated Dealing System (NDS) is an initiative, which provides for an electronic platform for facilitating trading in Government Securities and Money Market Instruments. The system has been operational for over a year now and the manner in which it has been used is laudable. The RBI has been actively fine-tuning the PDO-NDS system. Based on the feedback received, efforts will continue in this direction. The Securities Settlement System (SSS) will, in the near future, provide online depository services for the Government Securities.

ii. The Clearing Corporation of India Ltd., established at the behest of the Reserve Bank, has established itself as a central counterparty and is presently extending guaranteed settlement for trades done in the Government Securities Market and the Forex Market. The number of products launched by CCIL in its short duration of existence speaks volumes of both the CCIL and the financial sector. The forex trading platform, offered by CCIL, for taking care of the settlement of interbank rupee-US dollar deals, provides for a deep, liquid and transparent forex trading facility. This will help in improving market efficiency and integrity.

iii. Special EFT has been introduced to facilitate funds settlement on T + 0 bases thrice a day. This facility is available from 2500 bank branches located in 500 centers.

iv. Centralized Funds Management System: The Centralized Funds Management System (CFMS) which facilitates funds and treasury managers of commercial banks to obtain the consolidated and account-wise, centre-wise position of their balances with all the Deposit Accounts Departments of the RBI has been installed at the various RBI locations as also banks which were ready with the infrastructure for obtaining the data in a networked environment.

CFMS is also an initiative, which provides for a Centralized Funds Enquiry System to the treasury branches of the banks in the first phase and the Centralized Funds Transfer System in the second phase. This allows the banks to deploy optimal funds. In this regard, the funds enquiry module of CFMS can also be used as a mechanism for knowing account balances at various RBI locations. Further, CFMS is also expected to enable a near real time transfer of funds between various operative accounts in pursuance of a customer's day-to-day funds management exercise.

v. Structured Financial Messaging System: The Structured Financial Messaging System (SFMS), the messaging software riding on the INFINET, was implemented, during the year, under review. Providing for safe and secure communication, the SFMS was tested at three banks during a pilot phase spanning four months from November 2001. Subsequently, it was made operational in banks, which have provided the requisite infrastructure for SFMS effective January 2002. One of the key components of SFMS is security. Apart from smart card based access – an integral component of SFMS – the requirement of digital signatures has also been suitably addressed.

REAL TIME GROSS SETTLEMENT

Real Time Gross Settlement (RTGS) solution is a milestone in the saga of Indian payment system. It will enhance competitiveness within the system. It gears up the banks to meet future challenges posed by the external environment. RTGS system, if implemented with due precautions and proper action plan, will certainly help the Indian Banking Industry to attain global standards. The RBI has taken up many initiatives to establish an integrated payment and settlement system in the country. Real Time Gross Settlement Dealing System, Securities Settlement System etc., are some of the projects taken up by the RBI in this regard. The RBI also, through IDRBT is introducing structured financial messaging system to facilitate financial communication electronically on the lines of SWIFT. The RBI has given special focus on the implementation of the Systematically Important Payment System (SIPS) applications to facilitate interbank funds transfer in a secured environment. The Centralized Funds Management System, Negotiated Dealing System and Establishment of the Clearing Corporation of India Ltd. etc., are some of the initiatives taken by RBI towards SIPS. The securities settlement system will in the near future provide depositary services for the government securities including online real time payment and settlement for securities transactions. The working group on systemically important payment systems set-up by the RBI has identified the following payment systems:

i. The interbank clearing/high value clearing/MICR clearing

ii. Securities clearing and settlement system

iii. The government securities and foreign exchange clearing system

iv. The proposed real time gross settlement system.

RTGS is the ultimate in the payment and settlement architecture in any country primarily for online, real time interbank payment and settlement of large value funds. RTGS payment system can also be called as one in which payment instructions between banks are processed and settled individually and continuously throughout the day.

Working of RTGS System

Each participant of the RTGS will be required to open a dedicated settlement account for putting through its RTGS transactions. This account will be an intra-day account i.e., it would be operational only during the course of the RTGS day. The account will be funded at the start of the day (SOD) from a current account, which the participant holds under the present system at Deposit Account Department (DAD), RBI, Mumbai. Balances in the RTGS account at the end of the day of the RTGS day are swept back to participant's current account, thereby zeroing the RTGS account. The system enables the participants to place standing instructions with DAD, Mumbai to fund their RTGS account each morning duly specifying an actual amount or percentage of balance to be transferred to the RTGS settlement account everyday at SOD. The system also provides funds to the

RTGS account during the day from the participant's current account. Payment transactions emanating from a participant are ordinarily expected to be settled immediately after they are received which is the essence of the real time system. The proposed RTGS provides maintenance of participant-wise payment queues in which payment transactions will be held in first-in-first-out basis. However, to enable the participants to take care of the urgent time – critical payments and to enable more effective funds management, the system allows the participant to assign priorities to the payment messages and thereby, enables a particular transaction to be processed before another transaction, which was submitted earlier.

The system also provides facilities to the participants to view their respective transactions held in payment queues, to cancel such transactions and even change their priorities. However, participants can only view outgoing transactions on their own payment queues. They cannot view other participant's queues or their own pending incoming payment transactions. The system facilitates participant initiated movement of funds between various accounts held by it to optimize funds deployment and economize intra-day liquidity requirements. The proposed RTGS system provides a wide array of transaction types, which can be flexibly deployed to meet varying requirements. The system also provides interbank transactions types, which can be used to settle participant's financial obligations on their own account. The RTGS solution also provides for a separate transaction type, which can be used to transmit the customer information along with the payment message to the beneficiary's bank in a structured format. Delivery vs. Payment transactions from the RBI securities settlement system will also be settled in the RTGS system as a separate transaction type. To ensure smooth settlement of transactions it is imperative that participants ensure at the time of submission of payment instructions, that there are sufficient funds in their RTGS settlement account to settle their transactions as soon as they are submitted. The RTGS system enables provision of intra-day lines of credit by the RBI to the participants of the RTGS system in order to enable them to meet their intra-day liquidity in order arrangements. Such intra-day liquidity will be fully collateralized and will be provided to the participants at a charge per transaction. The RTGS solution acts as an optimized gridlock resolution tool to overcome crippling liquidity problems, which may be invoked periodically or at the discretion of the RBI to enable smooth settlement of RTGS transactions.

The multilateral net settlement batches i.e., the modified method of existing clearing batches will also be settled in RTGS system. This will ensure Net Clearing batches from the CCIL etc., in a more efficient manner.

Scope of RTGS

The scope of the settlement through RTGS extends to the following:

- Money market transactions
- Foreign exchange deals
- Capital market and debt instrument deals
- Funds settlement after securities auctioning
- Funds settlement after various interbank clearings
- Funds transfer between individual accounts of the same bank
- Funds transfer between individual accounts of different banks.

Issues in Implementation of RTGS

The new online settlement system that is increasing in membership numbers will raise many new issues in the implementation process of the service. As such, banks need to gear up themselves to meet the additional requirements that are suitable for the RTGS system. While doing so, they need to review and re-engineer their business processes to match the online interbank settlements. Banks will

learn to live without the float funds, which they enjoy in the present settlement system. Necessary infrastructure and tools need to be in place for individual banks to enable online liquidity management, which requires instant information and decisions. In the electronic payment processing environment, payment instructions are processed on continuous/real time basis and settled on gross/individual transaction basis without netting the debits against credits. Payments so effected are final and irrecoverable. The settlement is affected in the books of the RBI. RTGS enables banks and financial institutions that maintain accounts with the RBI to transfer funds from one account to the other, on their own or on customer's behalf, on an immediate, final and irrecoverable basis during the RTGS working hours.

Benefits of RTGS

For the Economy

- RTGS will reduce the systemic risk that exists in the present settlement systems, like cascading affect on banks due to failure of one bank to meet its settlement commitments.
- It improves confidence of outside agencies like World Bank on Indian Economy.
- It enables efficient settlements and avoids settlement delays.

For the Banks

- It offers immediate and irrecoverable settlement.
- It provides high-value intra-bank and interbank funds transfer.
- It provides new opportunities for formulation of innovative products.

For the Customers

- It provides sophisticated online banking services.
- It offers reliable high-value funds transfer.
- It improves personal image with beneficiary.

MICR

Magnetic Ink Character Recognition is a character recognition system that uses special ink and character. Any document, which contains this ink, needs to be read, and passed through a machine, which magnetizes the ink and then translates the magnetic information into characters. Banks mostly use MICR technology. The numbers and characters that are written at the bottom of the cheques are mainly printed with this ink. This requires a laser printer, which accepts this MICR toner. This provides secure, high-speed method of scanning and processing information.

Box 2: Payment Systems in ICICI Bank

Anywhere Banking

- Cheques issued payable at par at various ICICI Bank locations.
- Single account to be operated at any ICICI Bank branch for this facility.
- Ideal for small value, large volume payments.

Fund Transfers

- Online transfer of funds between accounts maintained with any branch of ICICI Bank.
- Issue of Bulk Demand Drafts/Pay Orders.
- Capability to issue Bulk Demand Drafts/Pay Orders on various ICICI Bank and correspondent bank locations.
- Capability to accept online requests from the customers.

- Capability to print beneficiary advice and dispatch.
- Remote printing facility.
- Simple process with a low turnaround time and delivery.

Cheque Writing

- Cheques can be issued on behalf of companies.
- Capability of processing large volumes of cheques in a short turnaround time.
- Capability of printing facsimile signatures.
- Capability to print beneficiary advice and dispatch.
- Ideal for bulk payments such as pension payments, gratuity payments.

At Par Payments

- Services can be availed for the 'at par' payment of dividend warrants/interest warrants/refund order/redemption payments/brokerage payments.
- Simplified and streamlined procedures ensuring smooth process flow online validation of instruments before payment. Regular reconciliation statements provided by the bank.
- Covering over 100 major locations through own network (90% of the payments). Arrangement with correspondent banks thereby covering over 200 locations through instruments based payments.
- ECS credit facility at all available locations.

Source: www.icicidirect.com

DEVELOPMENTS IN THE PAYMENT AND SETTLEMENT SYSTEMS

Recognizing the greater impetus ascribed towards payment and settlement systems, it was decided to assess the essential requirements for such systems, which impact the economy as a whole. These 'systemically important payment systems' are those, which have definitive impact on not only the entire payment system scenario, but also on the economy, in general. To assess the various issues arising out of such systems, an internal Working Group on Systemically Important Payment Systems was constituted to examine the various payment systems in vogue. The systemically important systems identified by the Group include the Interbank Clearing System, the High Value Cheque Clearing System, the MICR/Main Cheque Clearing, the Electronic Clearing System, the Electronic Fund Transfer System, and the Securities Clearing and Settlement Systems at Stock Exchanges. The RTGS system being implemented and the proposed Government Securities and Foreign Exchange Clearing and Settlement System were also identified as systemically important payment systems. The Group recommended that the RBI in respect of such systemically important payment systems should formulate general guidelines. Further, direct access to the RBI operated payment systems should be restricted only to banking entities, barring exceptions like Clearing Corporation of India Ltd., which have significant role in the payment and settlement systems. Moreover, all systemically important payment systems operated by other than the RBI should get their funds settled through any sponsor bank including the RBI. In order to facilitate banks to formulate their plans for implementing effective payment systems within their own area of activities, a Vision Document was published in December 2001. The document outlines the vision of the RBI in respect of payment and settlement systems for the immediate future and the medium term. The document indicates the broad framework of the initiatives being taken by the RBI and the approach adopted for time bound implementation of the various projects.

The payment systems in India have substantially evolved in recent years. These changes have had an impact on all types of payments – whether business-to-business or business-to-consumer. From the days of manual clearing operations, all the large business centers now have a Magnetic Ink Character Recognition (MICR) clearing process. The Reserve Bank of India (RBI) manages the clearing house at the key business centers and has been at the forefront in driving the initiatives towards a more electronic payment and clearing system. The first steps taken by the RBI were the introduction of the Electronic Clearing Service (ECS) in the mid-1990s that enabled electronic clearing of low-value, large-volume payments (e.g. dividends). ECS provided a four-day settlement cycle for low-value direct credits and direct debits. However, one of the key challenges to the growth of ECS payments in India has been the degree of automation in the Indian banking industry. While most private sector banks have networked branches with highly automated systems, many other banks have limited automation with little or no inter-branch connectivity. This results in a lack of "last-mile connectivity".

While the transactions are processed electronically at the clearing house, they are subsequently processed manually at the beneficiary banks, thereby largely obviating the benefits of an electronic settlement process. In spite of such issues, ECS is now quite popular in India for making large-volume payments, such as dividends. ECS was followed by the Electronic Funds Transfer (EFT) system. While participation in the EFT system was earlier restricted to state-owned banks; it was subsequently opened up to all banks. The EFT system enables an electronic transfer of funds inter-city and interbank, and is now available for high-value transfers as well. Recently, the RBI further enhanced the EFT system with the introduction of the Special Electronic Funds Transfer (SEFT) system, which is expected to facilitate the migration to T + 2 settlement in the securities market. The SEFT scheme provides for banks to define which of their branches will participate in the network, with the prerequisite that these branches be electronically linked with the coordinating branch in Mumbai, where all settlements take place. This system ensures that the beneficiary bank posts credits promptly, as the processing is electronic. SEFT should address, to a large extent, the issue of last-mile connectivity and is another step in moving India towards a more electronic payments mechanism. The RBI has defined a clear vision for the development of payment systems in the country, and EFT and SEFT are key building blocks for further technological developments. In addition to payment systems such as EFT and ECS, other payment mechanisms such as credit cards and debit cards are also gaining popularity in India. Many banks have recently started issuing debit cards with developments on smart cards; it is expected that their use will increase rapidly in India.

The role and importance of an effective payment system has been vindicated more by the recent turn of events in India. "Black Monday" has demonstrated to us the need and importance of an effective payments system that is real time. The importance of the implementation and operation of Real Time Gross Settlement System (RTGS) is picking up pace with Andhra Bank announcing on 19th May 2004 that it has also joined the system. An effective payment system acts as a mechanism for balancing the stability of the financial system, and naturally, such a payment system also influences the efficiency of the financial intermediaries, thereby influencing the pace of growth of the economy.

We now take a look at the importance, role and operation of the Clearing House, that in fact forms the backbone of the payments and settlements systems.

CLEARING HOUSE

Virtually countless number of transactions take place as business deals get settled every day in banks all over India. This is the reason why a clearing house is so important. When workers go on a strike, the clearing system comes to a grinding halt, whereby millions of transactions get affected. This ultimately affects the economy as a whole.

A clearinghouse in simple terms is a system that supports settlements through cheques or any other electronic methods of payment.

A clearing house basically carries out three main functions:

a. It registers and manages commitments resulting from market transactions (a back office function).

b. It provides a central counterparty role (a netting function).

c. It ensures integrity of its operations.

The objectives behind the setting up of a Clearing House in India are given below:

a. To make arrangements for the speedy and economic collection of cheques, bills and other documents payable or deliverable at or through offices of the members and sub-members of the House situated in the city/town by a system or systems of clearing with power to apply or to extend any system or systems to any place and from time to time abandon, re-constitute or alter any system or systems.

b. To make arrangements, and to frame rules relating to the collection or non-collection or documents between members and sub-members of the Clearing House.

c. To maintain records of the Clearing House and of such other matters as may be thought fit.

d. To draw up and prescribe from time to time forms for the use of the members and sub-members of the House in connection with the clearing.

e. To do all such other lawful things as are incidental or conducive to the attainment of all or any of the foregoing objects.

The Manager, Reserve Bank of India shall be the ex-officio President of the Bankers Clearing House. The President shall be the ultimate authority in managing the Clearing House.

Wherever the Reserve Bank of India (RBI) is willing to undertake the management of the Clearing House, or the State Bank of India (SBI) or one of its associates (as may be specified by the SBI) in the event of the RBI not undertaking the management, and in the absence of either, one of the public sector banks in that centre, which may be specified by the RBI, shall be the bank managing the Clearing House.

The President may, in the event of a temporary absence from duty, nominate another officer of his bank to act for him, and failing such nomination, the officer of the bank managing the Clearing House who is currently looking after the duties of the manager shall act as the President of the Clearing House during the period of such absence of the President.

The President will be assisted by a Standing Committee, constituted at a meeting of the members, in resolving the problems/issues/situations requiring urgent solutions.

The Standing Committee shall consist of not less than five, but not more than seven members, including the President, and will comprise:

i. The bank managing the Clearing House.

ii. The Reserve Bank of India wherever it is not managing the Clearing House and where it has its banking department.

iii. State Bank of India or any of its associate banks as may be specified by State Bank of India wherever they are not managing the Clearing House.

iv. The two other public sector banks where the Clearing House is managed by a bank other than the Reserve Bank of India or State Bank of India or its associates, and in other cases three other public sector banks, as may be specified by the bank managing the Clearing House.

v. Two other banks specified by the bank managing the Clearing House, from out of remaining members of the Clearing House.

The term of office of the member of the Standing Committee coming under categories (iv) and (v) shall be two years. The concerned member should nominate its representative, who will be participating in the meetings on behalf of the said member.

SUMMARY

- The payment and settlement systems are vital for the survival and growth of financial systems.
- In the present day context, various new types of instruments are merging mostly in the plastic and electronic forms that have made this system even more complex.
- Following this introduction, the risk factors for payments systems have been discussed. Considering the internationalization of payment systems, the International standards on payment systems that have evolved have been discussed.
- The Central Bank in every country is ultimately responsible for the successful operation of the system.
- In this regard, we also discuss about the role and concern of the Central Bank and the participants in the system. We also discuss about how this system actually operates in India.
- Further, the importance of quick settlements has resulted in the emergence of Real Time Gross Settlement (RTGS) whose structure, operations and benefits have been described in detail.

Chapter IX

Service Quality Metrics

After reading this chapter, you will be conversant with:

- Core Factors
- Customer Relationship Management
- Technical Quality and Functional Quality
- Role and Process Capability for Managing Services
- Managing Service Delivery
- ISO 9000 Certification in Banking Services

The banking industry worldwide has experienced remarkable changes over the last two decades. As a result, the global financial markets have undergone the process of major transformation. The changed environment has given more leverage to opening up the frontiers of operations by easing or removing altogether the existing restrictions. Consequently, the banking industry is under tremendous pressure to design new products, develop superior processes and implement structured solutions to complex financial problems. The fact is that an estimated $12 billion has been lost in the financial markets since 1992 which is attributed to poor risk management and fraud. Consequently, in 2001, the Basel Committee on Banking Supervision issued a second set of proposals – the New Capital Accord (Basel II). This was aimed to handle risk management throughout financial services. Basel II factors operational risk into the calculation of total capital requirements. This has widened the scope of the first Accord thereby impacting IT and operations departments within banks.

The IT operational risk issues raised by Basel II are addressed by utilizing standard risk management and quality improvement techniques from the Six Sigma quality management process. The IT services that support critical-to-quality business processes are defined. The potential risk of IT service failure is assessed, the cost of poor quality calculated, and measurements taken automatically to determine exposure to risk for any given moment. With such information available on hand, the banks are in a position to take the necessary steps to reduce risk and their capital provisions.

The focus of the banking sector has therefore shifted to such operational features as building operational efficiency and implement cost reduction programs. These results are to be achieved in the backdrop of more stringent regulatory environment and under more uncertain industry features such as mergers and acquisitions. In this scenario, IT has played a crucial and positive role.

In this process, the application of Real Time Enterprise (RTE) concept has become a competitive necessity. Gartner rates this as “critical to the financial service industry”. Thus, banks are now increasingly adopting RTE principles in their core business processes with the major objective of improving operational efficiency. The Business Activity Monitoring (BAM) capability that is developed by banks in the process helps to drastically reduce latency in operational decision-making. It is in this context that, service quality metrics help to improve the effectiveness of business operations by facilitating implementation of appropriate actions for dealing with problems.

In this exercise of improving operational efficiency and reducing costs, the ultimate objective has been to render effective customer service offering differing products and services suited to the customers’ requirements.

CORE FACTORS

We can list down a few core factors that have accelerated this process of bringing about what we may call as ‘financial innovations’ that have influenced the service quality metrics in the banking industry. These are as follows:

- Globalization of the financial markets
- Increased competition among the bankers
- Price volatility
- Regulatory and tax changes
- Interest rate volatility
- Exchange rate volatility.

John Finnerty said, “Financial engineering involves design, development and implementation of innovative financial instruments and processes and the

formulation of creative solutions to the problems in finance." Clearly, the key words are 'innovative' and 'creative'. To be creative and innovative may require a quantum leap in terms of acceptance and implementation of new ideas and systems. This could also mean that instead of implementing new ideas and systems, the existing products and services may only require slight modification to meet the new requirements.

There have been other versions regarding the role of financial engineering in delivering innovative products and services. Miller views financial engineering as an "unpredictable improvement in the variety of available financial products resulting from unforeseen changes." Kane views it from the perspective of regulatory dialectic.

According to Silber, the innovative financial instruments and processes are perceived as endeavors by corporations to mitigate the financial constraints they face. According to him, the cost of following the rules provides the impetus for innovative activities. Interestingly, this process relaxes the constraints and thereby reduces the cost of compliance. Van Horne takes a more critical view, maintaining that a new product or process cannot be considered 'truly' innovative unless it makes the financial markets operate more efficiently or makes them more complete. According to him, financial markets are made more complete by the introduction of new securities whose contingency after tax cash flows cannot be replicated by any combinations of existing securities.

The 'key factors' that drive innovations in products and services in the banking industry are given below:

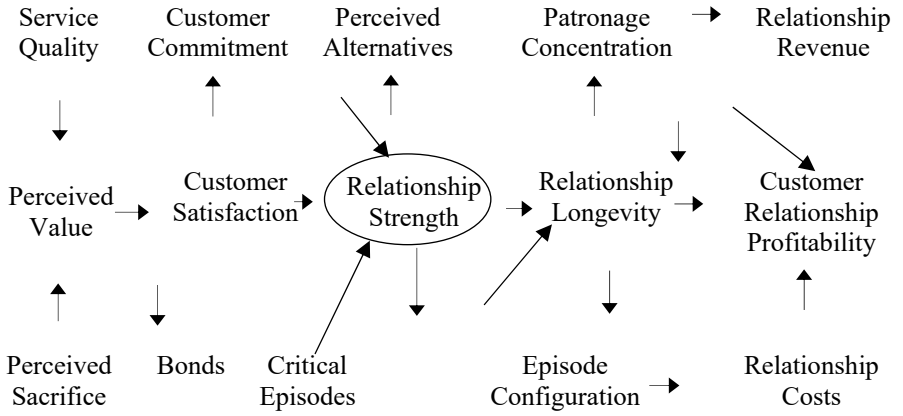
- Reduction in transaction costs
- Reduction in agency costs
- Time compliance
- Leveraging tax asymmetries
- Appropriate risk management strategies
- Adequate liquidity
- Regulatory compliance
- Leveraging of technology
- Innovations in financial management
- Arbitrage opportunities with many markets in existence.

We begin the discussion about service quality metrics by identifying the importance of CRM in terms of customers' demands and requirements and banks' responses to such stimulus.

CUSTOMER RELATIONSHIP MANAGEMENT

Customer relationship is the base on which the entire structure of banking rests. When we look at the cost and returns factor in building up customer-relationship management, we find that the initial cost to develop customer relationship is always higher than the revenue. However, as the relationship grows new demands will appear and then the incremental revenue would be higher than the incremental cost. This feature is demonstrated by figure 1. The costs associated with building up of a relationship are huge. They include – advertising costs, price incentives, set up costs for accounts, information and service costs etc.

Figure 1: A Relationship Profitability Model



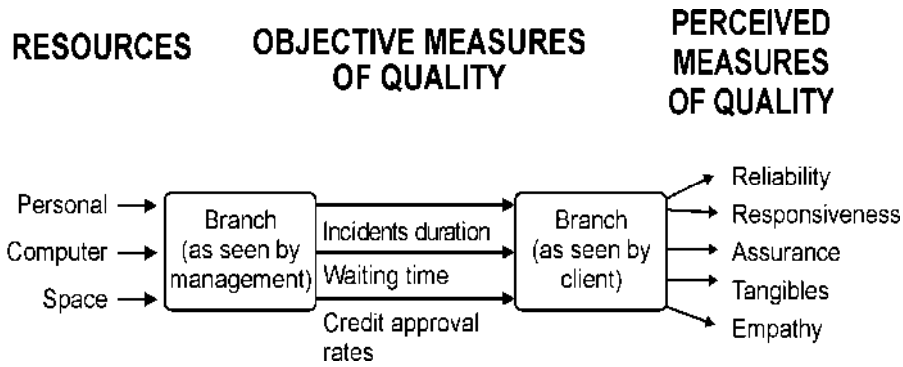
Source: Storbacka Strandwik and Gronroos, "Managing Customer Relationship for profit. "The Dynamics of Relationship Quality," International Journal of Service Industry Management, Vol 5. No.5.

On the cost front, the reality is that the banking industry needs to incur huge costs. Such costs are in the form of fixed costs, customer-driven costs, high relationship origination costs and considerable cost differences in serving the customers through the different distribution channels. The concept of services is complicated, as a service may encompass many features, ranging from a personal service involving a complex relationship to a service more like a commodity with a tangible product, and thus more easily comprehensible. An example of the latter is car rental, where the customer drives the car – a very tangible and comprehensible result of the service offered – whereas in the case of the former, using insurance services as an example, the customer pays for something highly impalpable, namely risk reduction. The insurance company bears the risk, which the customer consumes all the time. Customers, however, do not really comprehend the total context of the service until a loss is experienced.

Customer service delivery is vital for the success of banking. Use of technology to a great extent serves this purpose, but not entirely. It is equally important that the process consistency within and across service channels is maintained. Human resource policies are very important for improving process consistency. Thus, it can be said that service quality metrics as far as the customer is concerned are determined by a combination of three factors: alignment of technology, human resource management and strategy.

Hence, one of the major challenges that service managers face is *how* to deliver services of high quality. Branches ignoring service quality may report high volume of products and services offered, as well as profits, but lose their advantage in the long run due to eroding service quality. Quality efficiency in a bank can be measured as follows:

Figure 2: Quality Efficiency in a Bank



In the above figure, the 'perceived measure(s) of quality' is the final quality as seen by the customer. This can also be stated as the customers' perception of quality. There are five dimensions to the quality as perceived by the customer.

Box 1: Perceived Dimensions of Service Quality

- **Reliability:** The ability to perform the promised services accurately and dependably.
- **Responsiveness:** The willingness to help customers and provide prompt service.
- **Assurance:** The knowledge and courtesy of employees and their ability to convey trust and confidence.
- **Tangibles:** The appearance of physical facilities, equipment, personnel and communication materials.
- **Empathy:** The caring, individualized attention provided to the customer.

Quality Driven Performance

Quality thus drives performance. The service profit chain by Heskett, 1997 and the Service Management Model by Voss, 1997, imply that, quality drives performance. Today, the focus has been on customer-perceived quality, especially when dealing with service operations. Customer-perceived quality is the driver of banking operations. The service-profit chain of Heskett *et al.* (1994) clarifies the role of quality, and its interrelationships with operational aspects of a service organization.

The arguments in Heskett *et al.* proceed as follows:

i. Profit and growth are stimulated primarily by customer loyalty;

ii. Loyalty is a direct result of customer satisfaction;

iii. Satisfaction is largely influenced by the value of services provided to customers;

iv. Value is created by satisfied, loyal and productive employees;

v. Employee satisfaction results primarily from high-quality support services and policies that enable employees to deliver results to customers.

Figure 3
Service Profit Chain (Heskett *et al.,* 1994, 1997)

The Service Management Model (Voss *et al,* 1997)

While taking a look at the above models, it is important to note that there is no unique way for building these models. For example, when there is a mention about service quality, the following questions must be answered: Is quality with reference to customer perceived quality, or quality as determined by some objective measures (e.g., queue length and waiting time), or quality as perceived by the branch's management (internal customer perceptions)? As for profitability, is it the efficiency with which costs are transformed to profits, or does the management consider revenue growth as well?

We shall now discuss about the various banking services within the framework of Technical Quality and Functional Quality.

Box 2: Quality Matters
"Organizations today do not view their strength in enabling growth in terms of the quantity of management; the emphasis is on the quality of management," says Armand V Feigenbaum and Donald S Feigenbaum. In the highly demanding beginning years of the twenty-first century, many companies and business leaders have a quality of management that is a new competitive leadership combination of passion, populism, and disciplined responsibility. This quality of management has become a common denominator even though these companies and leaders may differ in their history, personality, evolution, and markets. It also is the basic foundation for capitalizing the management power.

TECHNICAL QUALITY AND FUNCTIONAL QUALITY

We revisit the importance of Technical Quality and Functional Quality in banks, which was covered in an earlier chapter, for the purpose of convenience. Service Quality in banking industry contains two components: (i) Technical quality, and (ii) Functional quality. Technical quality provides an answer to the question "what", i.e. giving the essence of the service itself, and it is objectively measurable. Functional quality represents an answer to the question "how." Here, it characterizes itself more closely with the manner by which a certain service has been provided and reflects the subjective perception of the consumer. While discussing about CRM in earlier pages we touched upon such issues. We include into technical quality such factors as, for example, the depth and width of the product range, know-how, and the possibility to use electronic banking. Therefore for a bank, *technical quality* refers to 'what' the bank gives the customer while *functional quality* refers to 'how' the bank's services are provided to the customer. Typical factors, which influence functional quality are: speed, courtesy, and in the case of electronic banking services in particular simple access and transparency. Both qualities are linked and together they create the final service quality of the bank in the backdrop of the image of the bank based on past customer relationship.

Since quality forms the basis of success or failure of a bank it is appropriate to know how quality parameters are arrived at as discussed in the following paragraphs.

Quality by Design

Quality by design can be defined as the quality inherent in a product due to its proper design and in the case of a manufacturing unit it is based on the processes used in producing a commodity. Quality by design is effective because it is the most effective way to improve quality. This is made possible by designing systems and standards to deliver quality. In banking parlance, the methods that the banks establish, the costs that the customer has to bear and the time norms within which the listed services can be obtained, are crucial components of quality by design.

It may be reiterated that, designing products and services that meet specific needs is very important. The basic premise of Quality by Design is that, at each phase, the process devotes careful attention to certain quality standards that prove critical to both the successful implementation of the process and the quality of the output. Quality by design has six aspects as follows:

i. **Usability:** The basic structure of the process should assist users in accomplishing their tasks efficiently and effectively.

ii. **Adaptability:** The structure should have the ability to easily and cheaply redesign existing functions for new processes, and should provide access to existing legacy information, and also provide a well-defined process for transition from the old processes to the new.

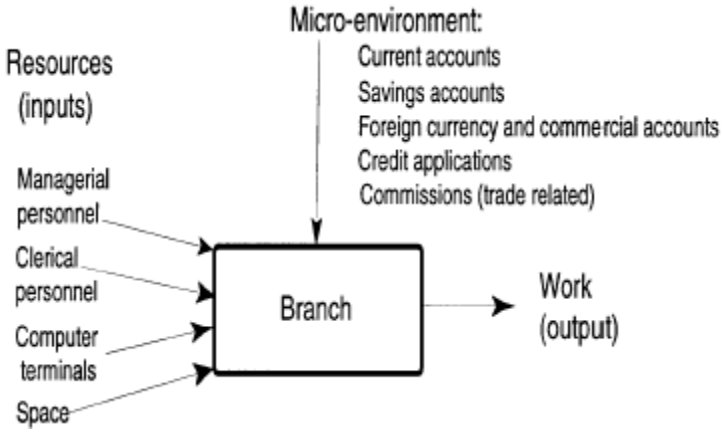
iii. **Manageability:** The system managers should be able to economically configure, monitor, diagnose, maintain, and control the resources of the environment in which the process is deployed.

iv. **Scalability:** The process should be designed in such a way that it should be able to efficiently handle any increasing load as it grows with the business needs.

v. **Security:** The process structure should have features of security built into them so as to protect confidential information and resources from unauthorized use. It should also have a monitoring system to check on the usage patterns and also report any form of discrepancy from the normal pattern.

vi. **Reliability:** The components of the architecture should be dependable for mission-critical business operations. Quality design of object classes and frameworks with an eye to maximize reuse can also increase the reliability of the resulting system.

Figure 4: The Inputs and Outputs of the Production Model for Benchmarking the Operational Efficiency of a Branch



One of the challenges that service managers face is *how* to deliver services of high quality. The benchmarking model in the figure above assists in identifying those branches of a bank that deliver superior quality services, and aid the rest in their quest for quality improvements. Most efficiency benchmark models developed for bank branches consider operating efficiency and/or profitability. Branches ignoring service quality may report high volume of products and services offered, as well as profits, but lose their advantage in the long run due to eroding service quality. The service managers must identify those branches that utilize their resources in the most efficient way to deliver high-quality to their clients.

The importance of achieving high-levels of quality has been discussed extensively, especially when dealing with the service industry. Service quality is considered by many as the key to gain competitive advantage, and its importance for the banking industry, in particular, has been documented in Roth and Van der Velde (1991, 1992). It is therefore difficult for a bank today that has not initiated some kind of service quality improvement program.

Quality Assurance

Quality assurance in banking can be defined as a formal methodology designed to assess the quality of banking services provided. Quality assurance includes formal review of care, problem identification, corrective actions to remedy any deficiencies and evaluation of actions taken. It can also be defined as the set of

activities that specifies acceptable material and process parameters and measures actual performance in meeting defined quality standards.

When used in reference to a department – Quality Assurance (QA) or Quality Control (QC) – often indicates that the responsibility for meeting quality standards has been delegated to that department, and is not an assumed function of other company operations.

To assure quality, the processes should be documented, institutionalized and evaluated. This will help in the structure becoming more effective and efficient as it is being used. Quality Control and Management principles should be applied to all aspects of the Execution, Delivery and Management cycle. Rigorous Quality Control and Management procedures should be put in place to minimize the number of 'defects'. Quality should be the path, not the destination.

Banks' approach to quality assurance as indicated above is visibly demonstrated in certain instances, and is also laid down as a code in their rule book. There are numerous examples in this regard. Cash payments at banks' counters, issue of a demand draft, issue of a cheque book, issue of a pass book, collection of cheques in clearing, collection of outstation cheques, processing of loan applications – all such activities are to be performed by banks within a time and structural framework.

Box 3: The Benefits of ISO 9000 Certification

ISO 9000 provides a framework and systematic approach to managing business processes to produce a product/service that conforms to customer expectations. For customers, the certification of suppliers to ISO standards means that they can be assured that the development of their products and services are compliant to reference documents that are globally accepted. This, of course, means that customers and suppliers are able to compete in markets around the world.

The benefits of becoming certified are numerous; companies should ensure that they are pursuing certification for the right reasons:

- To improve business processes and save money. Most companies implementing ISO 9000 Certification report increases in business process efficiencies, reduces waste, and improves product quality.
- To qualify for new customers. Many corporations target ISO 9000 Certification as an essential requirement for conducting business with a new vendor.
- To enter global markets. ISO 9000 standards are required in many countries.

Source: http://europe.isixsigma.com/library/content/c000917b.asp

ROLES AND PROCESS CAPABILITY FOR MANAGING SERVICES

In order to improve the quality of services further, it is essential to define services and agree upon the expected service quality levels that are necessary to meet business needs. Fundamental to this process, is the common understanding between the customer and service provider(s) of the customer's service expectations and the providers' capability.

There are a number of basic team roles encompassing service delivery and support activities.

Operational Level

Making end-users aware of the facilities available and how to exploit them to best effect is one of the responsibilities of the 'user-support' role.

Tactical Level

The 'service level management' role ensures that service quality monitors, based on service level agreements, are used as a basis for process/service improvements.

Higher level competencies that are required for 'managing services' build upon the operational and tactical capabilities described above. For example, the 'service management' role builds upon the service quality monitors established by 'service level management' and uses them to demonstrate ongoing value for money and service improvements. They are also responsible for establishing suitable baselines to track performance relating to service delivery and service improvement. The 'relationship management' team role is primarily responsible for removing barriers and opening gateways or communication channels between the customer and service providers. The role is one of listening to the various parties and understanding service expectations, positions and achievements.

The role plays a key part in managing the ongoing change and effect on the relationships between partners and providers. A key necessity is to understand and influence the factors which preserve and enhance relationships to achieve maximum business benefit.

The highest level designated in the team model for 'managing services' is represented by the 'business continuity' role. The role is primarily responsible for ensuring that, business continuity plans are kept up to date to reflect the criticality of operational services to the business and to reflect changes and new service provision.

Figure 5: Team Model for Managing Services

The team model includes:

i. **Service level management:** Using service level agreements as a basis for process/service improvement.

ii. **User support:** Making end-users aware of the facilities available and be able to exploit them to the best effect in support of their needs.

iii. **Requirements/Change management:** Monitoring the requirements of end-users and taking them into account during the ongoing development and delivery of services and systems.

iv. **Relationship management:** Managing relationships with providers at all levels including: strategic, service delivery and contractual levels.

v. **Service management:** Establishing suitable baselines on which to track performance relating to service delivery and capability improvement.

vi. **Business continuity:** Establishing an ongoing appraisal of risk and assuring that the necessary service components are recognized within business continuity plans; ensuring that business continuity measures are adequately tested.

With regard to banks, to improve role and process capability as mentioned above, managers specially designated for the purpose are recruited, trained and placed on the job. Depending upon the organizational structure that is in place, banks outsource some of the above services. At the tactical level, different types of banks like the public sector banks and private banks deploy permanent staff. However, at the operational level while public sector banks normally recruit permanent managers, there are a few private banks that utilize the services of agents for this purpose.

MANAGING SERVICE DELIVERY

We have discussed earlier that the methods that the banks establish, the costs that the customer has to bear and the time norms within which the customer can obtain the listed services, determine the customer's perception of the quality of services. To augment the capabilities of a bank, the following table deals with establishing such high service levels and also ensures that they are maintained. To maintain such service levels, striking a balance between quality and cost to ensure a value for money outcome is vital. During this phase, the risks should be managed and plans put into place to ensure business continuity should service failure or interruption occur.

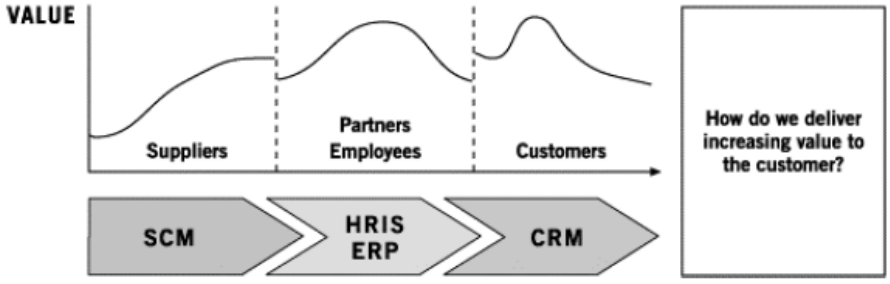
Table 1

What needs to be done to maintain service delivery	Points to be considered
Establish what levels of service are required, and ensure that they are maintained. Service level management is the process of managing the performance provided to the customer as specified in the contractual performance metrics. It balances cost and quality of services in order to provide the customer with value for money.	There should be a detailed agreement of the required service levels and thus the expected performance and quality of service to be delivered. Where the provider is an in-house department, the level of service required will be set out in a Service Level Agreement (SLA). Wherever there are formal agreements, on service levels as elsewhere, there is often a need for some flexibility. This is particularly true in the early stages of an agreement.
Measure quality as well as quantity. The quality of the service being delivered must be assessed. This means creating and using quality metrics - measurements that allow the quality of a service to be measured.	Quality measures might assess such aspects as completeness, availability, capacity, reliability, flexibility and timeliness, among others. Some aspects of a service may be measurable by numerical means; others may require subjective assessment.
Ensure Ensuring value for money is about the trade-off between service quality and cost. A key objective for the management of any contract is to ensure that it continues to achieve value for money over time.	Aim to optimise the ratio between value and cost. Realising that value for money is not synonymous with lowest cost. Carefully consider all the benefits that the contract provides in relation to the ongoing investment it requires. All costs associated with the contract must be taken into consideration: set-up costs, recurring costs, fixed costs, unit costs, and the organizations own overhead in managing the contract.

Compare prices and learn from others. Benchmarking is the practice of making like-for-like comparisons between organizations with the aim of ensuring continuing value for money, getting better performance, and improving business practices.	Price comparisons offer a quick and effective way to gauge whether you are getting value for money. Providers could be obliged to benchmark their own costs, or those of their subcontractors, by the contract. Compare the value for money you are getting with what other organizations are getting. Compare the way you manage contracts with the way other organizations manage theirs.
Manage the risks. Risk is defined as uncertainty of outcome, whether positive opportunity or negative threat. In the area of contract management, managing risk means identifying and controlling factors that may have an impact on fulfillment.	Risks can relate to many aspects of the contract, including fluctuation in demand, lack of provider capacity, change in requirement and transfer of skilled staff (on either side). All risks should be identified and managed. Risks should be placed with the party best placed to manage them – possibly the provider, although they will want compensation in return. Risks placed with the provider are referred to as 'transferred risks'. Business risk cannot be transferred to the provider. The final responsibility for achieving outcomes remains with the customer.
Ensure service continuity A major part of contract management is considering service continuity – what will happen if the service fails or is interrupted.	It will normally be the provider's responsibility to manage service continuity, and this will be stipulated in the contract but it will need to be taken into account in the organization's wider business continuity plan. Those aspects of a service identified as critical may require careful consideration and/or the creation of a Business Continuity Plan.

Organizations including banks have invested heavily in Supply Chain Management (SCM), Enterprise Resource Planning (ERP), Human Resources Information System (HRIS), and Customer Relationship Management (CRM) solutions to help drive business performance. There are a few critical observations in this regard. Firstly, improvements in business performance (revenue and profitability targets) are sustainable only if they result in increased value delivered to customers. Secondly, while these applications (SCM, CRM, ERP, etc.) focus on specific parts of the value chain, they focus only on the *management of embedded processes*. Thirdly, these applications fall short of enabling companies to manage and translate the wealth of intellectual capital around these processes into value ultimately delivered to customers. Fourthly, these applications also fail to address the varying nature of skills and knowledge needed for innovative problem solving and further enhancement of overall productivity. An organization could lose the wealth of intellectual capital around these processes if knowledge and learning are not actively managed across the enterprise to create value.

Figure 6: Delivering Value to Customers – What Helps?



Hence, to competitively deliver value to customers, value creation has to have its basis in the bank's internal intellectual capital. The skills of its employees, the product and/or service expertise developed internally, and the know-how embedded in its business processes form the core of that intellectual capital. The challenge, however, is creating an advantage out of this asset that is both competitive and sufficiently sustainable to impact the bank's business value drivers. Creating an advantage out of intellectual capital begins with enabling a culture of value creation: an environment where knowledge is captured, managed and disseminated along the value chain, with the main objective of giving employees, shareholders, government and the customers up to date skills and know-how in pursuit of increasing value to customers. By increasing value to the customer, the company enjoys greater adoption of its products and subsequently greater gains in the bottom line.

Box 4: What is the Future of ISO? ISO 9000:2000

The ISO 9000 family of quality management system standards, called ISO 9000:2000, is finally being updated. Why you ask? Well, it hasn't been updated since initially issued, and the committee agreed that it needs to reflect a more modern understanding of quality. On September 14, 2000, the standards took one further step towards finalization.

These new standards are now being distributed to the institutes that make ISO's worldwide membership. It will be approved if at least 75 percent of the votes cast on November 14, 2000, are in favor. In this case, it will be published as the new International Standards in December, 2000.

The three FDIS (Final Draft International Standards) which have just been published are the following:

- ISO/FDIS 9000, Quality management systems – Fundamentals and vocabulary
- ISO/FDIS 9001, Quality management systems – Requirements
- ISO/FDIS 9004, Quality management systems – Guidelines for performance improvements.

ISO 9000 CERTIFICATION IN BANKING SERVICES

The ISO and WTO have recognized the need to develop international standards for services. In this regard, Mr. Leopoldo Colombo, Head of the IRAM Systems Certification Department, has mentioned about the need for service sector to adapt to ISO 9000 standards to enhance their service capability and also to provide significant benefits to customers. ISO 9000. standards serve as an excellent tool for banks that have already undergone radical restructuring to meet the new demands of global markets, while at the same time ensuring a homogeneous service delivery throughout the world.

In this regard, the banks have to focus on two areas: Continuous improvement and customer satisfaction. This has to be done if the banks have to retain their competitive edge and remain profitable in the long-term. At the same time, the difficulties that are encountered by service organizations in general in the process of implementing a quality system according to ISO 9000, have also been recognized.

Among the different service sectors, the banking sector around the world has shown great interest in ISO 9000 certification.

As if to reiterate this fact, the RBI has decided to go in for a global quality certification. The concern of the RBI is to improve counter-related services and currency management, and streamline its process of regulation and supervision. According to the RBI, Deputy Governor, Ms K. J. Udeshi, the RBI to begin with will go in for an ISO 9000 certification for its currency management system. The reason behind this move is that as the regulator, the RBI is always to inclined towards internal scrutiny. Hence, it wants to be certified as being comparable to international standards.

While the RBI as the Central Bank of the country, has taken this initiative, the Indian banks have been urged to go in for ISO certification to standardize their systems and processes and improve the quality of their services.

Sensing the need of the hour, a number of banks have gone in for ISO certifications. The list of such banks includes Bank of Baroda, Punjab National Bank, HDFC Bank and IDBI Bank. The scope of certifications is varied though. The range of operations include general banking services related to deposits, loans and remittances and collection of cheques, to other forex and non-fund based activities. The banks have in fact become 'quality conscious'. This is proved by the fact that a number of banks are undertaking 'Six-Sigma' exercises to improve their operational performance. The banks that have already taken the lead in this regard are: the State Bank of India, ICICI Bank, HDFC Bank and Citibank. All in all, these developments should augur well for the 'king' who is none other than the customer.

SUMMARY

- The core factors providing quality services in banks have been discussed. The customer is the focal-point around which banking services are built. Hence, an exclusive section has been devoted to Customer Relationship Management. The quality of services that are offered in banks can broadly be categorized under Technical Quality and Functional Quality.
- The infrastructure in the form of managing service quality by specifying roles and incorporating process capability for managing services determines the extent of quality of services provided. The systems for managing service delivery have also been touched upon as also the concern of banking industry in obtaining ISO 9000 Certification.

Chapter X

Improving Quality and Productivity

After reading this chapter, you will be conversant with:

- Banking Services: Technical Quality and Functional Quality
- Determining What Satisfies the Customer
- Customers' Perception of Banking Service Quality
- Devising Quantitative Determinants
- Non-Quantitative Determinants
- Quality by Design: Formulating a Suitable Standard
- Quality Assurance
- Improving Productivity and Performance

The concept of services, its definition and scope have been discussed in detail in Chapter "Understanding Services" of this textbook. Progressing further, this chapter will deal with service quality and productivity of the services and measures to improve them.

Talking purely in terms of services, the services provided by a bank are only a part of the service spectrum. However, with the differences in an investment bank, commercial bank and insurance firm reducing, banks now offer a plethora of services. In India, even the NBFCs are offering commercial banking services and a commercial bank like Kotak Mahindra, for example, offering merchant banking services has been permitted by the RBI to offer commercial banking services while HDFC Bank and ICICI Bank offer merchant banking services.

Another differentiation is that of retail services and corporate services. Retail banks offer services involving the transfer, borrowing and lending of money to private customers and sole traders and partnerships. Commercial banks deal with corporate or commercial customers rather than individuals. Many of the major retail banks have commercial banking arms. Client size can range from small start up companies to major corporations.

BANKING SERVICES: TECHNICAL QUALITY AND FUNCTIONAL QUALITY

Service quality contains two components – Technical quality and functional quality. While technical quality provides an answer to the question "what", i.e., giving the essence of the service itself, and is objectively measurable, functional quality represents an answer to the question "how." Thus, it more closely characterizes the manner by which a certain service has been provided and reflects the subjective perception of the consumer. We include into technical quality such factors as, for example, the depth and width of the product range, know-how, and the possibility to use electronic banking. Therefore for a bank, *technical quality* refers to 'what' the bank gives the customer while *functional quality* refers to 'How' the bank's services are provided to the customer. Typical factors, which influence functional quality are: speed, courtesy, and in the case of electronic banking services in particular simple access and transparency. Both qualities are linked and together with the image of the given financial services provider, which represents a certain relationship of the past, these create the final service quality.

Technical Quality

To ensure that it delivers technical quality, the bank must ensure that

- Its products and services are closely aligned with customer needs.
- Customers are adequately informed about the bank's products and services.
- The bank's staff, especially front-line staff, has thorough knowledge of the bank's products and services.
- The bank's branch has a suitable mix of people with experience in banking, finance, accounting and legal aspects, so as to ensure that the branch is adequately equipped to deliver technical quality.
- The bank's staff is able to effectively communicate with customers- staff should also be able to converse in the local language, if required.
- The bank's staff is able to provide professional advice to its customers
- The bank's staff, especially frontline staff, has been adequately trained to deal with 'difficult' customers and with customer complaints.
- Handling of customer grievances is the overall responsibility of a senior official who not directly involved with the routine branch banking operations.

Functional Quality

Functional quality is concerned with how the service is provided to the bank's customers. A few elements that affect a banking service's functional quality include:

- Attitude of the bank's staff members
- Importance given to the bank's customers over routine work
- Perceived credibility of the bank's officials to customer queries
- Ambience at the bank
- Ability to hold discussions with senior officials.
- Image of the bank as a whole.

A bank must be equipped to deliver both technical and functional quality thus ensuring that it provides its customers with total quality service. Relevant qualitative determinants could be set up for a few technical and functional quality parameters, but most of these remain difficult to quantify. A bank could set up appropriate policies and procedures, for example, recruitment policies, to create enabling conditions for providing technical and functional quality to its customers. The ultimate focus should firmly be on providing quick and cost-effective quality banking services.

The 4 steps approach can go a long way in helping the bank achieve its quality goals. The steps are:

- Determining what satisfies the customer
- Customers' Perception of banking service quality
- Devising quantitative determinants and non-quantitative determinants
- Monitoring.

We look at each of these steps in a little greater detail.

DETERMINING WHAT SATISFIES THE CUSTOMER

This is the most crucial and perhaps, the most difficult part of the exercise. The best way to determine what satisfies the customer is to ask the customer. Several organizations regularly send out questionnaires and direct mailers to their customers (both internal and external), analyze the feedback received and initiate appropriate action.

CUSTOMERS' PERCEPTION OF BANKING SERVICE QUALITY

'Customers', who are central to the banking service, are not a homogeneous class. They come from varying socio-economic and cultural backgrounds. The perception of the quality of banking services provided will differ from customer to customer and even for the same customer at different points of time, depending on his the mood and mindset at a particular point of time. A customer who needs money and comes to an ATM on a Sunday to find that it is not working is likely to be much more dissatisfied than if she/he were to find the same ATM temporarily out of order on a working day. Some other factors that may influence perceptions of banking service quality are:

- Overall ambience at the bank.
- Past experiences with the bank.
- Familiarity with the services offered by the bank, the procedures followed etc.
- Knowledge of or experience with competitors' products and services.
- Banking with a particular bank may be regarded as a status symbol.
- Interaction with and/or opinions of other customers' rights etc.

These factors make the measurement of banking service quality difficult and subjective.

DEVISING QUANTITATIVE DETERMINANTS

Based on various feedback results and on the bank's internal research, a bank may devise suitable quantitative measures that can be tracked regularly. After the system of tracking has stabilized, suitable standards can be set. Interface with customers' results in several "perceptions" that must be handled every day. A bank must ensure that these result in total customer satisfaction. For example, a bank's *Customer Service Standards* may stipulate that all incoming phone calls be answered within three rings, all queries be attended to within five minutes, no call be transferred more than twice, all messages be recorded and communicated to the concerned person/department within thirty minutes, etc.

Today, it is estimated that there are over 1500 banking websites, with the growing importance of the Internet; banks will have to formulate standards for Internet interface also. These could be, for example, all queries to be answered on e-mail within 12 hours and to be followed up with written communication within 24 hours, etc. Where there is direct interface with the bank's employees, it must be ensured that all customers get a maximum sense of satisfaction. Many banks have set standards, for example, not more than three people should be waiting in a queue at any counter, all in queues should be deposed off in 3 minutes, all deposits should be accepted and receipt issued in 10 minutes, etc. A bank should attempt to formulate *Quantitative Determinants* to enable objective measurement of various parameters. A few quantitative determinants that could be used by a bank included in its retail banking, corporate segments are:

Retail Banking

Quantitative determinates could include, for example, the time taken to

- Accept a cash deposit
- Accept a cheque deposit
- Complete a cash withdrawal
- Complete a cheque withdrawal
- Act of an account-opening request
- Open an account (provided everything is in order)
- Issue a draft
- Issue a cheque book
- Issue an ATM card
- Issue an account statement
- Give a locker
- Update a passbook
- Clear an outstation cheque
- Answer routine customer queries account balance, cheque clearing status, interest rates etc.
- Answer other customer queries about forex rates, etc., which may require information from other departments.

This would also give the bank a fair account of the internal customer service standards prevailing at its branches

- Complete voucher checking and posting
- Sanction overdrafts
- Process consumer loans etc.

These are all time-based determinants; it may also be possible for a bank to devise cost-based determinants in some of the above cases. However, a cost based determinant is often highly dependent on other factors like positioning of the bank, additionally, it may inadvertently shift focus of the exercise.

Corporate Banking

Quantitative determinates could be, for example:

- Total time taken to process a loan application.
- Time required in disbursing a sanctioned facility.
- Time between the taking of the decision and it being conveyed to the concerned party.
- Number of questions/documents provided for a loan request to be processed.
- Time taken by the customer to access the correct person to the branch.
- Number of references made by the corporate office to the branch before an application can be processed.
- Number of days taken at the corporate office to process a proposal.
- Number of follow-up efforts made to recover loans from defaulters.

These could be compared and benchmarked against similar figures for competitors.

OTHER DETERMINANTS

Quantitative determinants in other crucial areas could include:

- Number of complaints received per period month, quarter, etc.
- Percentage of repeat complaints or complaints inadequately handled.
- Percentage of complaints pertaining to attitude of employees, transaction processing time, excessive charges, wrong debit entries etc.
- Percentage of ATM down time.
- Percentage of system down time, maintenance time, etc.
- Percentage of customer space to total space at the branches of the bank.
- Ratio of employee turnover at the bank to the industry average.
- Average number of training person – hours provided by the bank.
- Average number and volume of exceptions reported per period.

CUSTOMER COMPLAINTS

Generally, it is found that customer complaints relate to one of the following areas:

- Deposit accounts, non-payment of interest, fraudulent withdrawal, transfer of funds, wrong debits, etc.
- Delay in collection of cheques, drafts, etc.
- Non-issuance of duplicate drafts, etc.
- Grievance relating to remittances.
- Failure to honor or delay in honoring invoked, LCs guarantees etc.
- Delay in the sanctioning of loans and advances, charging of higher interest rates, etc.
- Miscellaneous complaints.

As can be seen, most of the complaints relate to retail banking transactions. A bank could find it advantageous to focus more attention on introducing quantitative determinants for retail banking areas.

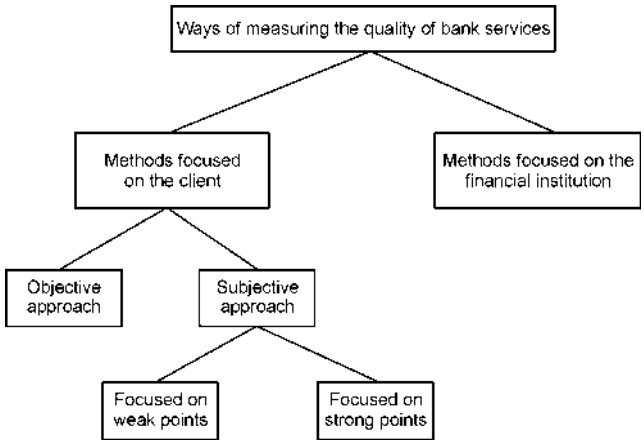
NON-QUANTITATIVE DETERMINANTS

A bank can also devise various non-quantitative determinants to help it improve its service quality. This is necessary because objective and scientific measurements may not always be feasible or practicable. Non-quantitative determinants can also throw additional light on various facets of the bank's service quality: Some of the areas a bank can focus on include branch premises and customer lounges, ATMs, technology, publicity, and staff members.

Non-quantitative determinants are often difficult to standardize or benchmark. In some cases, however, internal guidelines standardize ATM premises, branch premises, handling of customer complaints, questionnaires used to obtain feedback, etc. Many factors, like the customers, orientation of staff members may be difficult to evaluate and standardize. Recruiting policies and procedures to ensure that the right kinds of people are selected. The bank could also experiment with various tests – psychological tests, studying behavior in relation to a group, etc., to help it select the right person. As the validity and efficiency of these tests is often hotly debated, the bank must use them with caution and after careful analysis. The bank should then evolve suitable training programs to ensure that there is no effort lacking on the bank's part in equipping the selected candidates to perform their duties satisfactorily.

Non-quantitative determinants are very important because there is no mechanism to gauge where the bank went wrong. There will normally be no complaints relating to these factors, except if the staff has been extremely callous or rude. The effect of these factors on the customers' perception of quality is also difficult to ascertain. Further, the divergence in customer perception (as discussed already) is more pronounced for these non-quantitative determinants compared to the quantitative determinants. It is therefore important for a bank to pay adequate attention and attempt to reasonably standardize these factors with the focus being on providing timely and cost-effective quality services.

Figure 1:Measuring Quality of Bank Services



Source: www.nds.sk

As competition increases, quality will become the only true differentiator in services. Successful banks will compete on quality. Banks must realize that competing on price means that they are dependent on what the competition is doing, for their success. Competing on quality means staying ahead of the competition. Banks that wish to surge ahead successfully into the new millennium would need to ingrain a quality culture. Every aspect of the bank's functioning would have to be governed by the quality principles.

MONITORING

Once determinants have been set and standards have been devised, continuous measurement should be made to monitor progress. Quality Control Charts can be used to ensure regular tracking and any significant deviations are to be reported to the top management to get them rectified. Thus, suitable quantitative measures and policies should be designed to sustain continuous quality improvement in all areas of functioning.

Designing of Service Quality

Services have a number of distinctive characteristics, which differentiate them from goods and have implications for the manner in which they are marketed. These characteristics are often described as intangibility, inseparability, variability, perishability and the inability to own a service. The following are the four most commonly attributed characteristics of services:

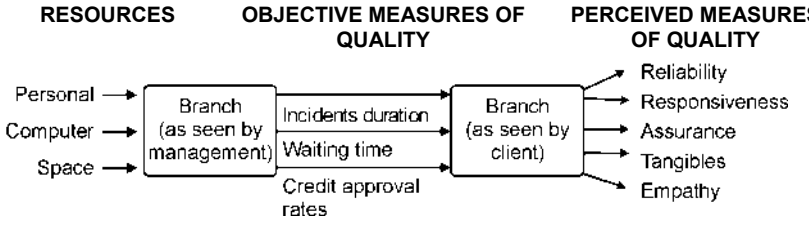
- Intangibility
- Inseparability
- Heterogeneity
- Pershability.

The above four have been discussed in greater detail in Chapter "Understanding Services". Another aspect which plays and important part in the design of service quality is the customer's perception of service quality.

CUSTOMER'S PERCEPTION OF QUALITY

One of the challenges that service managers face is how to deliver services of high quality. Branches ignoring service quality may report high volume of products and services offered, as well as profits, but lose their advantage in the long-run due to eroding service quality. Quality efficiency in a bank can be measured as follows:

Figure 2 : Customers' Perception of Quality



Source: www.ttra.com/pub/uploads.

In the above figure, the 'perceived measures of quality' is the final quality as seen by the customer. This can also be stated as the customers' perception of quality. There are five dimensions to the quality as perceived by the customer.

Box 1: Perceived Dimensions of Service Quality
• **Reliability:** The ability to perform the promised services accurately and dependably.
• **Responsiveness:** The willingness to help customers and provide prompt service.
• **Assurance:** The knowledge and courtesy of employees and their ability to convey trust and confidence.
• **Tangibles:** The appearance of physical facilities, equipment, personnel and communication materials.
• **Empathy:** The caring, individualized attention provided to the customer.

Source: www.ttra.com/pub/uploads.

QUALITY BY DESIGN: FORMULATING A SUITABLE STANDARD

Quality by design can be defined as the quality inherent in a product due to its proper design and the manufacturing processes used in producing it. Quality by design is the most effective way to improve quality. When the systems and standards are designed to deliver quality, the philosophy of quality which says that "quality is free" can be easily achieved.

Finding the correct balance between feature benefits is important to all customers. Designing products and services that meet specific needs is very important. The basic premise of quality by design is that, at each phase, the process devotes careful attention to certain quality standards that prove critical to both the successful implementation of the process and the quality of the output. Quality by design has the following six aspects:

i. **Usability:** The basic structure of the process should assist users in accomplishing their tasks efficiently and effectively.

ii. **Adaptability:** The structure should have the ability to easily and cheaply redesign existing functions for new processes, and should provide access to existing legacy information, and also provide a well-defined process for transition from the old processes to the new.

iii. **Manageability:** The system managers should be able to economically configure, monitor, diagnose, maintain, and control the resources of the environment in which the process is deployed.

iv. **Scalability:** The process should be designed in such a way that it should be able to efficiently handle any increasing load as it grows with the business needs.

v. **Security:** The process structure should have features of security built into it so as to protect confidential information and resources from unauthorized use. It should also have a monitoring system to check on the usage patterns and also report any form of discrepancy in the normal pattern.

vi. **Reliability:** The components of the architecture should be dependable at times of mission-critical business operations. Quality design of object classes and frameworks with an eye to maximize reuse can also increase the reliability of the resulting system.

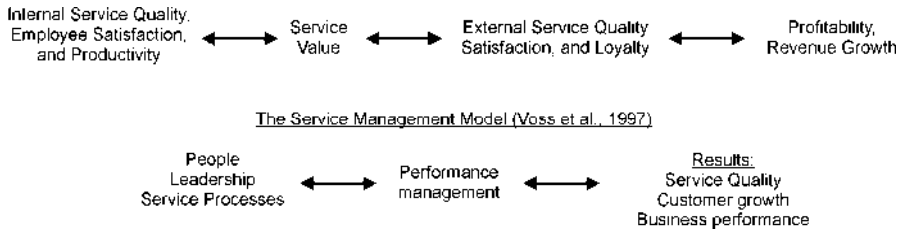
Quality-driven Performance

The service profit chain by Heskett, and the Service Management Model by Voss, 1997, imply that, quality drives performance. Today the focus is on customer-perceived quality, especially when dealing with service operations. Customer-perceived quality is the driver of retail banking. The service-profit chain of Heskett *et al*. clarifies the role of quality, and its interrelationships with operational aspects of a service organization.

The argument in Heskett *et al*. proceeds as follows:

- Profit and growth are stimulated primarily by customer loyalty;
- Loyalty is a direct result of customer satisfaction;
- Satisfaction is largely influenced by the value of services provided to customers;
- Value is created by satisfied, loyal and productive employees;
- Employee satisfaction results primarily from high-quality support services and policies that enable employees to deliver results to customers.

Figure 3: Service Profit Chain

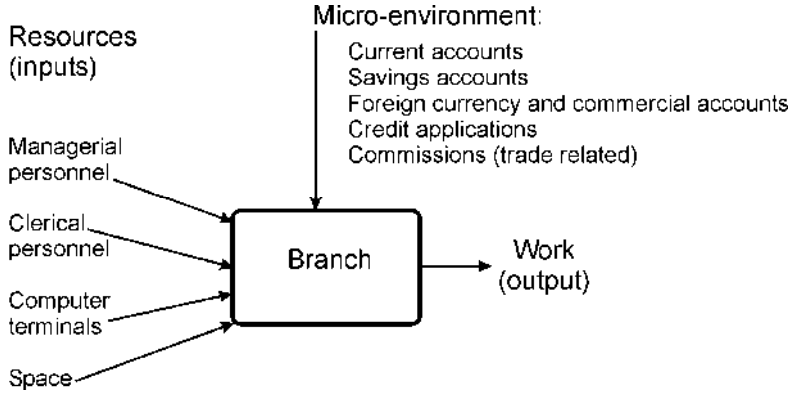


Source: The Service Profit Chain – J.L. Heskett, W.E. Sasser and L.A. Schlesinger.

While taking a look at the above models, it is important to note that there is no unique way to build them. For example, when there is a mention about service quality, the following questions must be answered: Is quality with reference to customer perceived quality, or quality as determined by some objective measures (e.g., queue length and waiting time), or quality as perceived by the branch's management (internal customer perceptions)? As for profitability, is it the efficiency with which costs are transformed to profits, or does the management consider revenue growth as well?

The importance of achieving high levels of quality has been discussed extensively, especially when dealing with the service industry. Service quality is considered by many as the key to gaining competitive advantage, and its importance for the banking industry, in particular, has been documented in Roth and Van der Velde (1991, 1992). It is difficult to find today a bank that has not initiated some kind of service quality improvement program.

Figure 4: The Inputs and Outputs of the Production Model for Benchmarking the Operational Efficiency of a Branch



Source: www3.gartner.com

One of the challenges that service managers face is *how* to deliver services of high quality. The benchmarking model in the above figure assists in identifying those branches of a bank that deliver superior quality, and aid the rest in their quest for quality improvements. Most efficiency benchmark models developed for bank branches consider operating efficiency and/or profitability. Branches ignoring service quality may report high volume of products and services offered, as well as profits, but lose their advantage in the long run due to eroding service quality. The service managers must identify those branches that utilize most efficiently their resources to deliver high-quality to their clients.

QUALITY ASSURANCE

Quality assurance can be defined as a formal methodology designed to assess the quality of services provided. Quality assurance includes formal review of care, problem identification, corrective actions to remedy any deficiencies and evaluation of actions taken. It can also be defined as the set of activities that specifies acceptable material and process parameters and measures actual performance in meeting defined quality standards.

When used in reference to a department – Quality Assurance (QA) or Quality Control (QC), often indicates that the responsibility for meeting quality standards has been delegated to that department, and is not an assumed function of other company operations.

To assure quality, the processes should be documented, institutionalized and evaluated. This will help in the structure becoming more effective and efficient as it is being used. Quality Control and Management principles should be applied to all aspects of the Execution, Delivery and Management cycle. Rigorous Quality Control and Management principles should be put in place to minimize the number of 'defects'. Quality should be the path, not the destination.

Roles and Process Capability for Managing Services

To achieve better quality services, it is essential to define services and agree upon the expected service quality levels that are necessary to meet business needs. Fundamental to this process, is gaining a common understanding between the customer's service expectations and the providers' capability.

There are a number of basic team roles encompassing service delivery and support activities.

OPERATIONAL LEVEL

Making end-users aware of the facilities available and how to exploit them to the best effect is one of the responsibilities of the 'user support' role.

TACTICAL LEVEL

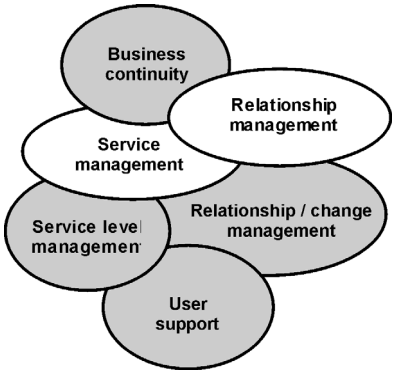
The 'service level management' role ensures that service quality monitors, based on Service Level Agreements, are used as a basis for process/service improvements.

Higher level competencies that are required for 'managing services' build upon the operational and tactical capabilities described above. For example, the 'service management' role builds upon the service quality monitors established by 'service level management' and uses them to demonstrate ongoing value for money and service improvements. They are also responsible for establishing suitable baselines on which to track performance relating to service delivery and service improvement. The 'relationship management' team role is primarily responsible for removing barriers and opening gateways or communication channels between the customer and service providers. Here, the role is to listen to the various parties and understanding service expectations, positions and achievements.

The role plays a key part in managing the ongoing change and effect on the relationships between partners and providers. A key outcome is to understand and influence the factors which preserve and enhance relationships to achieve maximum business benefit.

The highest level designated in the team model for 'managing services' is represented by the 'business continuity' role. This role is primarily responsible for ensuring that, Business Continuity plans are kept up to date to reflect the criticality of operational services to the business and to reflect changes and new service provision.

Figure 5: Team Model for Managing Services



Source: www.ogc.gov.uk/sdtoolkit/images/figs/page6(1).gif

The Team Model Includes

- **Service level management:** Using service level agreements as a basis for process/service improvement.
- **User support:** Making end-users aware of the facilities available and exploit them to the best effect.
- **Requirements/Change management:** Monitoring the requirements of end-users and taking them into account during the ongoing development and delivery of services and systems.
- **Relationship management:** Managing relationships with providers at all levels including strategic, service delivery and contractual levels.
- **Service management:** Establishing suitable baselines on which to track performance relating to service delivery and capability improvement.
- **Business continuity:** Establishing an ongoing appraisal of risk and assuring that the necessary service components are recognised within business continuity plans; ensuring that business continuity measures are adequately tested.

IMPORVING PRODUCTIVITY AND PERFORMANCE

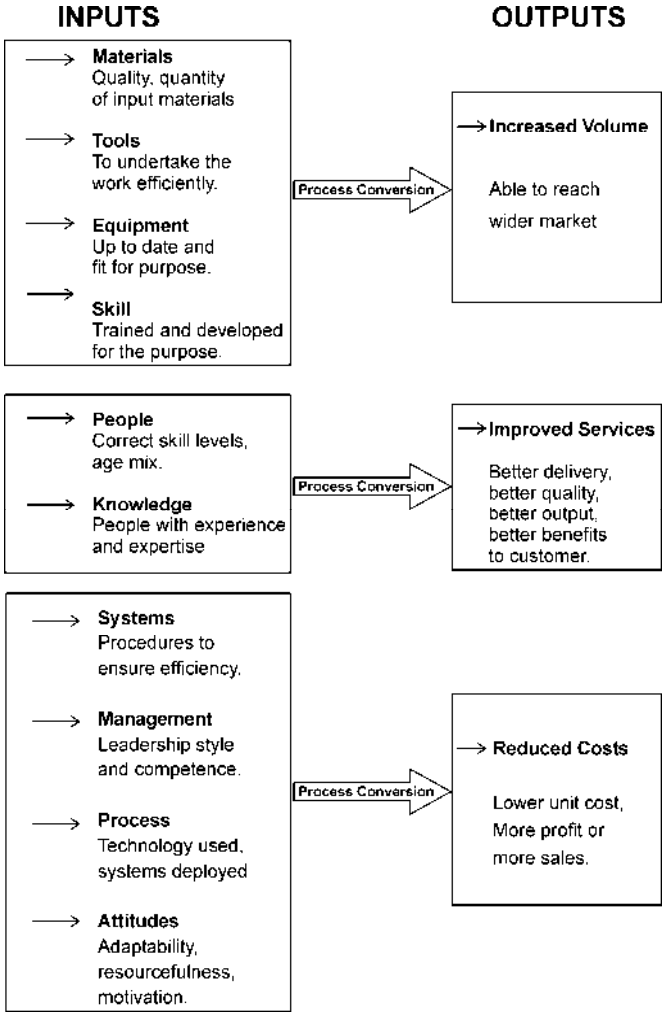
Productivity can be defined as: The output of any production process, per unit of input. To increase productivity means to produce more with less. In factories and corporations, productivity is a measure of the ability to create goods and services from a given amount of labor, capital, materials, land, resources, knowledge, time, or any combination of these.

To remain competitive in today's market place, organizations must look at ways to improve productivity. Improving productivity not only means looking at employee performance, but also means looking at technology and how well it addresses productivity of the employee. An employee cannot be productive if he or she cannot work or communicate while on the road or at remote locations.

Before one can improve productivity, one needs to know exactly what productivity is. Productivity can be explained by using a 'productivity tree'. Essentially, productivity is a ratio to measure how well an organization (or individual, industry, country) converts input resources (labor, materials, machines etc.) into goods and services.

This is usually expressed in ratios of inputs to outputs. That is (input) cost per (output) good/service unit. It is not a measure of how efficient the conversion process is. The Productivity Conceptual Model below, takes the form of a 'productivity tree'. The roots denote the inputs to the system, the trunk is the conversion process and the foliage and fruits are the system's outputs.

Figure 7: Productivity Conceptual Model



Source: Adapted from http://www.accel-team.com/productivity/productivity_01_what.html

The successful management of this process is ultimately the key to survival of any organization. It should be the concern of and a development goal for, all organizational members, irrespective of their position.

Improving Performance

Performance can be defined in two ways. One is the way in which an individual, group, or organization carries out or accomplishes its important functions or processes. Second, as a prerequisite to productivity, it is defined as follows: A major factor in determining the overall productivity of a system, performance is primarily tied to availability, throughput and response time. Thus both productivity and performance are interrelated.

Profitability and Productivity in Indian Banks

The Indian banking system has long been facing the challenge of lower levels of profitability and higher levels of NPAs, but, with the thrust now being on structural reforms and better risk management systems, Indian banks are definitely showing a lot of improvement. The combined average growth in net profits of public sectors banks for the year 2003-04 has risen by 59.5% and the average growth of advances has been 19% for the public sector banks and 26.3% for the private sector banks. The NPAs have also shown encouraging trends. The advent of E-banking and risk management systems have a role to play in the profitability of banks.

The credit quality of the Indian banking industry is benefiting from the reforms initiated by the Government over the years. The risk profile of Indian banks' loan

books has also eased gradually. The absolute level of NPAs in the Indian banks fell 3.0 percent and 4.0 percent during 2002-03 and 2003-04 respectively; this was due to stricter classification for the impaired assets, high treasury profits, which allows banks to write-off their bad debt more aggressively and also allows a higher level of debt restructuring.

Box 3: Best Year Ever for Indian Banks

By several commonly accepted measures – profitability, capital adequacy, level of non-performing assets – Indian banks have achieved their best levels of performance ever in 2002-03. While acknowledging this, many will say, "Oh, it's only on account of treasury income."

For years, foreign banks used to show huge profits derived overwhelmingly from the securities market. They were applauded as angels of efficiency. In those days, treasury was a neglected function at Indian banks. Well, times have changed. Indian banks have woken up to the potential of treasury income, so why grudge them the results they are showing?

The RBI's Report on Trend and Progress in Banking (2002-03) shows that, for banks as a whole, trading profits were significant in 2002-03, accounting, as they did, for 44% of operating profit but their importance varied among the various bank groups. The ratio was highest for old and new private sector banks (58% and 63% respectively) and lowest for foreign banks (14%), with the SBI group (30%) and nationalized banks (56%) coming in between.

The scheduled commercial banks showed a net profit to total assets of 1%, a much coveted figure internationally. It is not widely grasped that the Indian banking system, dominated by the much-maligned PSBs, is among the most profitable in the world. The Report has a table that shows that the post-tax return on assets of 0.75% of Indian banks in 2002 was higher than the pre-tax return of banks in a range of industrial economies except the United States.

Also noteworthy is that the intermediation costs in the Indian banking system, said to be one of its major failings despite deregulation, are lower than in five of the nine industrial economies mentioned in the Report. And significantly, intermediation costs as a proportion of total assets (3.46%) are the highest in the most profitable banking system in the world, the US, way above Indian costs of 2.19%. This raises the question whether intermediation costs should not be viewed in conjunction in overall profitability.

If high intermediation costs are compatible with a high-level of profitability, the former should not be an issue – unless it can be shown that high profitability results from lack of competition. This is emphatically not true of Indian banking. The level of competition, as measured by the share of the five largest banks in total banking assets, compares favorably with that in Asian, Latin American and industrial economies.

If there is one catch in the proposition that things are hunky-dory in Indian banking, it is that, thanks to the state of capital markets in recent years, disintermediation has not been a credible threat to Indian banks. For one thing, depositors are not fleeing to capital market-related instruments. The Report makes much of the fact that the spread of 2.8% in 2002-03 was lower than that of 3.1% in 1995-96 but this is a highly selective comparison. The spread in 2002-03 was higher than in the previous year (2.57%) and also the average in the initial years of deregulation, 1992-95 (2.72%). This is because, while lending rates have declined, banks have been able to push deposit rates even lower as savers lack an appetite for instruments other than bank deposits.

Indian banks have not been stretched on the lending side either as borrowers, by and large, do not have recourse to the capital markets. Indeed, banks' approach to managing credit risk has been to simply avoid taking risks with small borrowers. American banks, in contrast, went on to improve their performance in the teeth of competition from capital markets and by making a conspicuous success of small business lending. The true test for Indian banks thus still lies ahead but a decade of reforms has left them singularly well placed to face it.

Source: http://economictimes.indiatimes.com/articleshow/338125.cms.

Though the new generation private sector banks and foreign banks already had asset/liability management systems in place, it was learning time for the public sector banks and the old generation private sector banks. Credit must be given to these two segments of banks for despite the lack of proper MIS (backed by inadequate technology) and culture (of working under a risk management system) brave efforts have been made to unlearn and relearn managing interest rate risks through asset/liability management systems.

Risk Management

For the last two years, the Central Bank is trying to usher the Indian banking system towards a "Risk-Based Supervision System", however, with limited success. Again, the new generation private sector banks and the foreign banks were ahead of the systems, in the sense that the foreign banks had already well laid out risk management systems in place, and whereas the new generation private sector banks started their banking with such systems in place. The difficulty of the other two banking sectors, namely the public sector and the old generation private sector was the work-culture, internal systems and procedure and the mindset, which all needed a change in view of the Central Bank's objectives of ushering a "risk-based supervisory system." Progress in these banks, is painfully slow. Slowing down of the economy will make the situation worse, as some of the risk management systems like credit risk, will come under severe test.

Information Technology – Onset of E-Banking

Information Technology (IT) has wide ramifications for an entire gamut of issues concerning the banking sector. The growing internationalization of banking operations necessitates flexibility in financial policies to raise and sustain economic growth. Seamless integration of applications and systems is crucial to ensure smooth passage of interrelated transactions over the electronic medium for facilitating greater integration of various markets. Developments in IT have contributed to devising complex financial products, such as, derivatives, which in turn, have expanded the options for both savers and investors, in terms of asset preferences and risk profiles. Coupled with improvements in communications infrastructure, this is expected to give rise to efficiency advantage over a period.

In India, while the pace of technological upgradation would need to be accelerated to attain international standards, large investment requirements of the IT sector, particularly in banking, often act as an impediment towards undertaking full-fledged computerization of branches. It would be useful if banks devise a roadmap for networking 'critical offices', defined in terms of their volume, diversity and scope of work, so as to ensure coverage of a certain minimum quantum of business, with customer service as the main focus in the medium-term. Secondly, under the payment system, claims to various parties are interlinked which create potential risk problems, especially if the systems are too 'open'. As a result, smooth functioning of the payments system requires the integration of work processes, communication linkages and integrated delivery systems with focus on stability, efficiency and security. While adopting the relevant security standards for India, the specific requirements of the Indian banking system would need to be kept in view. Finally, to enhance further appreciation of IT applications, banks would need to proactively address issues that help set-up an efficient MIS through adoption of modern IT methods. To ensure sustained use of IT, institution of appropriate systems and procedures in commercial banks, and effecting requisite shifts from the written manuals to manuals in electronic form, would be imperative.

Banks – The Need for Quality Management Systems

The IITs find it worthwhile to go in for Quality Management Systems. A newly established engineering college in Bangalore achieved the miraculous distinction in its rating only through the adoption of quality regime. It is time hence to take

bank's quality management too in earnest. However, not many banks in India seem to have established Quality Management Systems. This is due to an impression, that in financial service, quality issues do not matter, as they do in manufacturing.

According to the ISO 9001:2001 standards, the *raison d'etre* of a quality management system is customer delight.

- Customer focus on a dynamic basis
- Continuous improvements through measurement, analysis and monitoring
- Business process development
- Standardization of work
- Accountability.

Of late, banking in India seems to be taking to Quality Management. The ICICI Bank has adopted the Six Sigma Approach – one of the sophisticated proactive techniques for bringing efficiency in service. Canara Bank adopted the ISO System for some of its branches and offices. While some of the Indian banks have adopted the ISO system generally, such quality systems and ratings have been confined to the branches. The major factor responsible for the neglect of quality management system in banking may be lack of clarity about the concept of quality and its implementation. Perhaps, the other banks have not adopted QMS on an enterprise-wide scale, due to certain apprehensions as:

The Quality Management System like ISO standards is applicable mainly to manufacturing entities and is not material for service organizations. The ISO Certification is important only for international trade and does not have relevance for domestic operations. The quality system implementation and certification is an additional work without significant benefits – it increases paper work enormously; the quality systems require extensive documentation of procedures and therefore, create operational rigidities and consequential delays and deterioration in reforms.

The above-mentioned apprehensions, perhaps, have been responsible for the lack of sufficient interest on the part of banks in the quality management system. However, this perceived irrelevance/inadequacies/absence of benefits from the quality management system will be found incorrect on verification.

The basic thing about Quality Management System is that it sets up customer delight as the central point of focus for all the operations of an organization. Secondly, it provides the framework to measure performance at the macro level and requires continuous improvements. A registration system like ISO would additionally require external validation of conformity of working of the organization and its procedures and practices to the mission, the goals and the regulations already set out. In fact, as the ISO 9001:2001 standards declare that the quality standards do not suggest and even imply, "uniformity in the structure of quality management system or uniformity of documentation like ISO do not prescribe and allow for the development of a unique customized quality system for each organization, according to its need and purposes and appropriate to its line of business, size and structure of the organization and scale of its operations."

However, the process approach advocated by the ISO 2000 standards for adoption by firms seeks to enhance customer satisfaction by meeting customer requirements. According to the standards, the process is defined as "an activity using resources and managed to enable the transformation of inputs into outputs". The scope of quality management system according to ISO 9001:2000 is "to demonstrate its ability to consistently provide a product that meets customer and regulatory requirements". Naturally, the international standards are generic benchmarks.

The ISO Quality Management System is customer-centric. In fact, the standards define the product itself as that "intended for, or required by the customer". Such a

System emphasizes continual improvement in the processes for value maximization. It advocates the methodology of Plan-Do-Check-Act (PDCA) for every one of the processes. The ISO 9000-2000 is the Certification standard which specifies the minimum requirements. The ISO 9004:2000 is wider in scope and lays down requirements for the pursuit of continual improvement in performance.

The 2000 ISO standards series covers all activities of the organization. Resource management including human resources, design and development of products, design and development and verification, production and service provision, validation of processes of production and service provision, control of production, service provision, identification and traceability, measurement, analysis and improvement and provision for continuous improvement through corrective action and preventive action are the main features of the model quality management system as envisaged in the ISO 9001:2000 standards.

As competition is hotting up, the key differentiation is going to be quality of service, which is going to determine the fate of the organizations and survival of the institutions. Setting out the processes in detail with clarity enables an organization to ensure that the service being provided or the product being delivered is of the kind that satisfies the customer. Quality system ensures consistency and objectivity in operations. However, it also provides for the exercise of judgment and qualitative decision-making wherever such processes are provided for.

Existence of external validation for the conformity of the organization with its processes ensures independent review and enables timely corrections. The framework of continuous improvement imposed on the organization by the quality system will push the organization at various levels right from the lowest to the highest to innovate and turn in measurable improvements in performance.

The major issues involved in implementing quality management system in banks are business process analysis, change management and automation. While the quality management systems do not require automation of business process analysis, the mission of customer delight makes them unavoidable. In fact, the implementation of quality systems in banks would mean wholesale transformation of the organization into a customer driven, technology-savvy and value-delivering entity. The key prerequisite for the implementation of such systems is leadership with vision, top management commitment and debt management. As process changes typically affect vested interests in the organization the strategic decision to go in for quality systems needs to be sustained by unambiguous commitment of the top management. The benefits are going to be greater customer mind share, market share, money share and profit share.

SUMMARY

- The quality of service that banks provide is vital to their survival. Another aspect is the productivity of the bank. A four step approach to quality where the bank determines what the customer needs, and devises quantitative and non-quantitative determinants of quality to suit the customers' varying tastes will help the bank in achieving its quality goals. While designing a service, though form follows function, the implications of service intangibility must be kept in mind. The profit chain designed by Heskett, shows how quality can drive performance.
- After defining the process, a quality assurance methodology must be defined to ensure the constant maintenance of the service quality. For this, the roles and process managing capabilities must be defined at both operational and tactical levels. The productivity conceptual model will help determine the outputs based on the inputs and how productivity can be improved.
- The chapter also deals with the aspect of quality in the Indian context, looking at the spreads and asset-liability managements and other ratios which help in determining the quality and performance of the banks. The need for quality management systems in Indian banks and the ISO certifications for certain banks have been also discussed.

Chapter XI

Operational Controls

After reading this chapter, you will be conversant with:

- Banking Regulations and Supervision
- Maintenance of Documents and Records
- Adequate Information Storage and Retrieval Mechanism
- Maintenance of CRAR
- Reporting
- Asset-Liability Management System
- Organizational Structure
- Audit and Vigilance

The sources of operational controls that are exercised in banks can be broadly categorized as – external sources of control and internal sources of control. In the Indian banking scenario, the external source of operational control is vested with the RBI, which formulates, implements and reviews the guidelines framed in this regard from time to time. Regarding internal controls, banks have to devise various mechanisms to exercise such control. They are:

i. Maintenance of Documents and Records

ii. Adequate Information Storage and Retrieval Mechanism

iii. Maintenance of CRAR

iv. Asset-Liability Management System

v. Organizational Structure

vi. Audit and Vigilance.

In this chapter, we begin a discussion about operational controls by referring to the RBI's banking regulations. This is followed by a discussion in detail about the systems and methods that are the banks have to implement by way of maintaining registers and ledgers. Since the advent of computerization in banks, the data storage and retrieval mechanisms are taking electronic form. Technology is fast displacing the traditional methods of banking emphasizing the need to be aware of information storage and retrieval. The recent developments in the banking sector supported by the RBI's guidelines in this regard, make it imperative to discuss about CRAR and the exercise of managing operations in banks which boils down to an exercise of Asset-Liability management. In this regard, we have discussed about the systems for effective implementation of these regulatory prescriptions. The mechanism of exercising operational control is possible only with a sound structure in place. Hence, the relevance of organization structure in operational controls has been brought to the fore. Lastly, the activity of Audit and Vigilance rounds up the operational control activities in the banking system.

BANKING REGULATIONS AND SUPERVISION

The separation of the regulatory and the supervisory roles of the RBI began with the setting up of the Department of Supervision (DoS) by the RBI in December 1993. The DoS has been set-up with its Central Office at Mumbai and 16 regional offices at various centers. This was followed by the establishment of a separate Board for Supervision (BFS) in November 1994. BFS aims at a dedicated and integrated supervision of overall credit institutions including banks, DFIs and other finance companies.

The Board for Financial Supervision (BFS) now provides undivided and intensive focus to prudential supervision. Apart from reviewing and revamping the existing supervisory strategies, the BFS has also put in place additional instruments of supervision to supplement the periodic inspections. The supervisory function includes verification of the capital adequacy and liquidity, the management practices, the presence of adequate systems and controls and compliance with laws and regulations. This verification process, follows two approaches:

i. On-site verification

ii. Off-site monitoring and surveillance.

The on-site verification involves examination of the books of accounts of the bank by the officials of the BFS or by external auditors.

To support the on-site verification, the DoS introduced in March 1996 the off-site monitoring and surveillance mechanism. This monitoring is based on the prudential reporting system and banks are required to furnish various reports to the RBI on a quarterly basis.

Financial markets are different from product markets. Therefore, greater liberalization should be there along with deeper supervision and higher degree of regulation. This is because financial institutions are more leveraged and there is more scope for speculative activities in such assets, given their inherent volatility. Moreover, there are negative externalities that can destabilize financial markets and this instability can adversely affect the real economy. Keeping the above aspects in mind, the RBI has instituted a three-pronged supervisory strategy comprising of on-site inspection, off-site surveillance and external auditing towards monitoring the health profile of individual institutions. The inspection for domestic banks is conducted in a more objective manner under the CAMELS (Capital Adequacy, Asset Quality, Management, Earnings, Liquidity and Systems) methodology and a comprehensive rating system has also been put in place. The banks have been advised about the procedure followed in the rating exercise in the interest of transparency and to help them in their efforts to improve their rating in the subsequent period.

With the passage of time, financial sector supervision is expected to become increasingly risk oriented and concerned more with validation of systems. There is a growing acceptance that Risk-Based Supervision (RBS) approach would be more efficient than the traditional transaction-based approach.

By virtue of the above-mentioned powers of the Reserve Bank, the operations and the operating environment of the banking sector are regulated and supervised. In addition to these, the RBI also exercises its control over the volume of credit created by the commercial banks, ensures price stability and the stability of the Indian currency vis-à-vis external currencies.

Box 1: Risk-Based Supervision (RBS)

The RBS process entails monitoring of banks by allocating supervisory resources and focusing supervisory attention according to the risk profile of each institution. The instruments of RBS are off-site monitoring and on-site examination supplemented by market intelligence mechanism. Internationally, off-site surveillance, however, gained primacy in recent times, given the ease and promptness of monitoring.

The objective of the RBS entails the allocation of scarce supervisory resources and paying supervisory attention in accordance with the risk profile of the concerned institution. This approach is expected to optimize utilization of supervisory resources and minimize the impact of crisis situation in the financial system. The RBS process essentially involves continuous monitoring and evaluation of the risk profiles of the supervised institutions in relation to their business strategy and exposure. Apart from strengthening the risk modeling capabilities based on off-site data and associated research for 'predictive supervision,' it would rationalize the overall compliance burden.

The major elements of RBS approach comprise of: (a) risk profiling of banks, (b) supervisory cycle, (c) supervisory program, (d) inspection process, (e) review, evaluation and follow-up, (f) monitorable action plan, (g) supervisory organization, (h) enforcement process and incentive framework, (i) role of external auditors, and (j) change management implications.

The central plank for RBS would be the risk profiling of banks, which, in essence, would document the various financial and non-financial risks confronting the bank. The risk profile of each bank, in turn, would entail drawing up of a supervisory program for the concerned institution, which would be flexible enough to permit amendments warranted by subsequent major developments. The supervisory follow-up process will seek to ensure that banks take timely corrective action to remedy or mitigate any significant risks

that have been identified in course of supervision. This would be implemented through the Monitorable Action Plan (MAP) that would not only outline remedial actions, but also link these to the areas of high-risk identified in the risk profiling and supervisory process. In order to make the framework incentive compatible, banks with better compliance record and good risk management and control system could be subject to a longer supervisory cycle and less supervisory intervention. In case banks fail to show improvements in response to the MAP, there would be a disincentive package comprising of more frequent supervisory examination and higher supervisory intervention such as directions, sanctions and penalties, including the mandatory and discretionary actions as enshrined in the Prompt Corrective Action (PCA) framework. The process would be supplanted by leveraging the use of external auditors by widening the range of tasks and activities performed by them. Since the success of the entire process would hinge critically upon the proactive response of banks, it is essential that banks have well-defined standards of corporate governance and documented policies and practices in place so as to clearly demarcate the lines of responsibility and accountability.

RBS offers several advantages. First, it enables supervisors to gain a better understanding of the quality of management, characteristics of the business and the risk a bank faces. It also enables supervisory authorities to display more consistency in carrying out supervisory responsibilities and establish best practices in the supervision of banks. Second, the explicit linking of tools of supervision to areas of risk or concern means that banks' management is better able to appreciate why a supervisor has used a particular supervisory tool. Third, in view of the high transactions costs involved in on-site supervision process, RBS will be better placed to decide the intensity of the future supervision, having obtained a better understanding of the bank's risk profile. The intensity of supervision and the amount and focus of supervisory action will increase in line with the perceived risk profile of the bank.

In India, in order to develop an overall plan for moving towards RBS, international consultants were appointed with the assistance of the Department for International Development of the United Kingdom. They have completed Phase-I of the project by conducting a review and evaluation of the current supervisory and regulatory framework, policies, guidelines, instructions, tools, techniques, systems, available IT infrastructure and external linkages. The thrust of Phase-I recommendations is on the enhancement of the regulatory and supervisory framework leading to the increased effectiveness of overall supervision through greater focus on risk as well as realignment of the inspection process with a more risk-based approach. The recommendations cover areas such as data management, supervisory process, inspection, feedback to banks, external audit, etc. During Phase-II of the project, the consultants are expected to work out the practical and operational aspects of the above recommendations and suggest a new RBS framework including the sequencing of different stages and a time frame for implementation. A dedicated group has been set-up within the RBI for project implementation and to drive the change management implication. To meet the requirements of RBS, banks would be required to take immediate measures to improve the reliability and robustness of their risk management, management information and supervisory reporting systems. The compilation of supervision manual for the use of supervisors is in progress and the RBS approach is scheduled to be operationalized during 2003.

Source: Trend in Banking/wwww.rbi.org.

MAINTENANCE OF DOCUMENTS AND RECORDS

At the bank/branch level, the basic structure on which the entire control mechanism rests is on the basis of the registers/ledgers that are maintained. These records form the basis on which data is generated for subsequent analysis in decision-making, be it for credit decisions, income-expenditure decisions or for that matter any decision in the course of operations. A list of such registers/records is given below, that in a way forms the prime basis for recording the operations in a bank/branch.

The documents of original entry and records of transactions must be adequate so as to show the correct entries of all transactions. The important aspects to be considered are:

i. Security items such as demand drafts, fixed deposit receipts, cheque books etc., should be stored as numbered items with due entries of storage and uses of such instruments being recorded.

ii. Documents should preferably be prepared at the same time when the transaction takes place.

The maintenance of documents and records should be such that the following information can be obtained as and when required:

i. Due records of all transactions.

ii. Identification and measurement of transaction values.

iii. Appropriate classification of transactions for reporting purposes.

iv. Facilitation in the presentation of the financial statements for the required time periods.

Books of Accounts

A broad classification of the books of accounts of a bank are as follows:

- Principal Books of Accounts
- Subsidiary Books
- Other Subsidiary Registers
- Other Memoranda Books
- Statistical Books.

Details relating to the recording of transactions in the various books of accounts are provided below.

PRINCIPAL BOOKS OF ACCOUNTS

The Principal Books of Accounts of a bank consists of the General Ledger and the Profit and Loss Ledger.

General Ledger

It contains all personal ledgers accounts, profit and loss accounts and different asset accounts. Balance sheet can be readily prepared from the general ledger. Contra accounts, which have no direct effect on the bank's position are kept with a view to control such transactions as letters of credit opened, bills received or sent for collection, guarantees given etc.

Profit and Loss ledger

Some banks maintain separate detailed profit and loss accounts other than the one maintained in the general ledger. These are columnar books having separate columns for each revenue or expense head. Some banks maintain separate books for debits and credits. Posting in these books is done directly from the vouchers.

The total of debits and credits posted are entered into the Profit and Loss account in the general ledger. Some banks maintain revenue accounts in the general ledgers itself, while other banks maintain broad revenue heads in the general ledger and its details in subsidiary ledgers.

SUBSIDIARY BOOKS

Apart from the principal books, there are subsidiary books maintained in the form of Personal Ledgers and Bills Registers.

Personal Ledgers

Department ledgers for different types of accounts, for example, Current Accounts, Fixed Deposits, Cash Certificates, Loans, Overdrafts, etc., are maintained by the bank. These ledgers are directly posted from the vouchers and all the vouchers entered in each ledger in a day are summarized into voucher summary sheets.

The voucher summary sheets are prepared in the department in which the transaction originates by persons other than those who write the ledgers. They are subsequently checked by persons generally unconnected with writing the ledgers on the voucher summary sheets.

Bills Registers

Details of different types of bills like bills purchased, inward bills for collection, outward bills for collection, are entered on a day-to-day basis in separate registers. Party-wise details of bills purchased or discounted are kept in normal ledger form. Entries in this register are made from the original document. A voucher prepared for the total amount of the transaction each day is entered in the Day Book. When a bill is returned or realized its original entry in the register is marked off. A daily summary of such realizations or returns is prepared in a separate register whose totals are taken to the vouchers, which are posted in the day book. Contra vouchers reflecting both sides of the transactions are prepared at the time of the original entry in respect of bills for collections, and this is reversed on realization. Outstanding entries are summarized frequently, and their total is agreed with the balance of the respective control accounts in the General Ledger.

OTHER SUBSIDIARY REGISTERS

There are different registers for various types of transactions. Their actual number, volume and details will vary according to the requirements of the bank.

The following are some such registers:

i. Bills for Collection Register
ii. Demand Draft Register
iii. Share Security Register
iv. Jewelry Register
v. Safe Custody Register
vi. Letters of Credit Register
vii. Safe Deposit Vault Register
viii. Standing Order Register
ix. Letter of Guarantee Register.

Entries into these registers are made from original documents, which are also summarized on vouchers everyday, and these vouchers are posted in the Day Book.

Departmental Journals

A journal is maintained by each department of the bank to note the transfer entries passed by it. These journals are only memoranda books, as all the entries made therein are also made in the day book through voucher summary sheets. Their purpose is to maintain a record of all the transfer entries originated by each

department. Two vouchers are usually made for each transaction by transfer entry, one for debit and the other for credit. The vouchers are generally made by and entered into the journal of the department, which is affording credit to the other department.

OTHER MEMORANDA BOOKS

Besides the books mentioned above, various departments of the bank maintain a number of memoranda books to facilitate their work.

Some of the important books are:

Cash Department

The main cash book is maintained by persons other than the cashiers. The important books maintained in the cash department are – receiving cashiers cash book, paying cashiers cash book, main cash book, and cash balance book.

Quick Payment System

To ensure quick service, banks have introduced teller system. The teller maintains cash as well as ledger cards and the specimen signature cards of each customer in respect of Current and Saving Bank Accounts. A teller is authorized to make payment up to a particular amount, say, Rs.8,000. On receipt of a cheque he/she checks it, passes it for payment, makes payment to the customer and enters it in the ledger card. The teller also receives cash deposited in these accounts.

Outward Clearing

A Clearing Cheque Received Book is for entering cheques received from customers for clearing.

Inward Clearing

Cheques received are checked with the accompanying lists. They are then sent to the concerned department, and the number of cheques given to each department is noted down in a Memo Book. When the cheques are passed and posted into ledgers, their number is independently verified with the Memo Book. If any cheques are unpayable, they are returned to the clearing house. The cheques themselves serve as vouchers.

Loans and Overdraft Department

i. Registers for shares and other securities held on behalf of each customer.

ii. Summary books of securities giving details of government securities, shares of individual companies.

iii. Godown registers maintained by the godown keepers of the bank.

iv. Price register giving the wholesale price of the commodities pledged with the bank.

v. Overdraft sanction register.

vi. Drawing power book.

vii. Delivery order book.

viii. Storage book.

Deposits Department

a. Account opening and closing register.

b. Rate register for fixed deposits giving analysis of deposits according to rates.

c. Due date diary.

d. Specimen signature book.

Establishment Department

a. Salary and allied registers, such as attendance register, leave register, overtime register.
b. Register of fixed assets.
c. Stationery register.
d. Old records register.

General

- Signature book of bank officers.
- Private telegraphic code and cyphers.

STATISTICAL BOOKS

Statistical records are kept by the banks as per their requirements. Some of the common books that are maintained are:

- For average balances in loans and advances.
- Deposits.
- Number of cheques paid.
- Number of cheques, bills and other items collected.

All the above-mentioned assets and records should be kept under the control of personnel duly authorized for this purpose. Surprise verification of the assets should be conducted. Through physical controls, access to tangible assets, which include cash and securities is generally restricted. Such controls can be in the form of physical limitations, dual custody, and periodic inventories.

ADEQUATE INFORMATION STORAGE AND RETRIEVAL MECHANISM

While the above-mentioned records are typical in relation to a manually-operated branch of a bank, it is nevertheless necessary that the hardcopies of all information be stored even with computerization of bank branches. Hence, the above information is valid in a fully-computerized branch as well, since the above-mentioned records are generated, printed and stored. However, apart from the storage of such printouts, the information that is available in the computerized system should also be appropriately stored and be retrievable as and when required.

Thus, the systems that hold and use data in an electronic form must be secure, monitored independently and supported by adequate contingency arrangements. It is in this context that the maintenance of a bank's management information system is so important. Hence, banks need to implement the organizational and management control requirements related to processing information in an electronic form and also need to have an adequate audit trail.

If the systems are poorly designed and controlled then it could affect the quality of decision-making. The electronic information systems have such risks that banks must effectively control. This is particularly needed so as to avoid disruptions to business and potential losses. Since transaction processing and business applications have expanded beyond the use of mainframe computer environments to distributed systems for mission critical business functions, the magnitude of risks also has expanded. Controls over information systems and technology should include both general and application controls.

The general controls are controls over computer systems (mainframe, client/server, and end-user workstations) that seek to ensure their continued, proper operation. General controls also include in-house back-up and recovery procedures, software development and acquisition policies, maintenance (change control) procedures, and physical/logical access security controls. Application controls are computerized steps within software applications and other manual procedures that control the processing of transactions and business activities. Application controls

include, operations such as, edit checks and specific logical access controls unique to a business system. In the absence of adequate controls over information systems and technology, the banks will be under threat of loss of data and programs. Such risks get magnified due to reasons such as inadequate physical and electronic security arrangements, equipment or systems failures, and inadequate in-house back-up and recovery procedures.

The next aspect of operational control would dwell upon the importance of adequacy of capital and quality of assets.

MAINTENANCE OF CRAR

To assess the adequacy of capital based on the quality of assets, the Capital to Risk-Weighted Assets Ratio (CRAR) or the Capital Adequacy Ratio (CAR) is now being focused upon. Introduced in 1988 by the Basel Capital Adequacy Accord, this ratio has become the keyword to comment on the stability of a bank.

As banking began to spread across nations and competition began to heat up among banks from varied countries, it became an unfair game for banks from the countries imposing stricter capital standards, as they will be at a competitive disadvantage. Therefore, a need for uniform capital standards for banks was felt. As a result, regulators from 13 countries including the US came together to formulate uniform standards that would apply to all the banks. These standards, established under the auspices of the Bank for International Settlements (BIS), an international clearing bank for central banks, were adopted in November 1988. The committee has adopted weighted risk assets approach, which assigns weights to both on and off-balance sheet exposures of a bank according to the perceived risk. The banking supervisory authorities in the G-10 countries apply this framework. The committee has suggested that the banking supervisory authorities of the non-G-10 countries could also try to adopt the framework, particularly, in respect of banks conducting significant international business in their jurisdictions. Internationally, capital adequacy has gained credence with the move towards the adoption of the new capital accord in place of the old accord given in 1988.

After assessing the capital funds and the risk-weighted assets, the bank will have to compute the ratio of the capital to risk weighted assets. The minimum CRAR was initially set at 8 percent. However, to meet the international standards, this has been raised to 9 percent with effect from March 31, 2000. At the end of March 2002, as many as 25 Public Sector Banks (PSBs) had CRAR exceeding the stipulated minimum of 9 percent.

REPORTING

Banks should furnish an annual return commencing from the year ended March 31, 1992, indicating:

a. Capital funds

b. Conversion of off-balance sheet/non-funded exposures

c. Calculation of risk-weighted assets

d. Calculation of capital funds ratio.

The format for the returns is given as a break-up and the aggregate in respect of domestic and overseas operations will have to be furnished. The returns should be signed by two officials who are authorized to sign the statutory returns submitted to the RBI.

ASSET-LIABILITY MANAGEMENT SYSTEM

In the normal course, FIs are exposed to credit and market risks in view of the asset-liability transformation. Liberalization of Indian financial markets over the last few years and growing integration of domestic markets with external markets, the risks, particularly the market risks, associated with FIs operations have become

complex and large, requiring strategic management. FIs are operating in a fairly deregulated environment and are required to determine interest rates on various products in their liabilities and assets portfolios, both in domestic as well as foreign currencies, on a dynamic basis. Intense competition for business involving both the assets and liabilities, together with increasing volatility in the domestic interest rates as also in foreign exchange rates, has brought pressure on the management of FIs to maintain a good balance amongst spreads, profitability and long-term viability. These pressures call for structured and comprehensive measures for institutionalizing an integrated risk management system and not just *ad hoc* action. The FIs are exposed to several major risks in the course of their business and are generally classified as credit risk, market risk and operational risk, which underline the need for effective risk management systems in FIs. The FIs need to address these risks in a structured manner by upgrading the quality of their risk management and adopting more comprehensive ALM practices than has been done hitherto.

The envisaged ALM system seeks to introduce a formalized framework for management of market risks through measuring, monitoring and managing liquidity, exchange rate and interest rate risks of an FI that need to be closely integrated with the FI's business strategy. This note lays down broad guidelines for FIs in respect of liquidity, exchange rate and interest rate risk management systems, which form part of the ALM function. The initial focus of the ALM function would be to enforce discipline in market risk management viz. managing business after assessing the market risks involved. The objective of a good risk management systems should be to evolve into a strategic tool for effective management of FIs.

The ALM process rests on three pillars:

- ALM Information System
  - Management Information System
  - Information availability, accuracy, adequacy and expediency
- ALM Organization
  - Structure and responsibilities
  - Level of top management involvement
- ALM Process
  - Risk parameters
  - `– Risk identification
  - Risk measurement
  - Risk management
  - Risk policies and tolerance levels.

ALM Information System

ALM has to be supported by a management philosophy, which clearly specifies the risk policies and tolerance limits. This framework needs to be built on sound methodology with necessary supporting information system, as the central element of the entire ALM exercise is the availability of adequate and accurate information with experience. Thus, information is the key to the ALM process. There are various methods prevalent worldwide for measuring risks. These range from the simple gap statement to extremely sophisticated and data intensive risk-adjusted profitability measurement methods. The present guidelines would require comparatively simpler information system for generating liquidity gap and interest rate gap reports.

ALM Organization

Successful implementation of the risk management process would require strong commitment on the part of the senior management in the FI, to integrate basic operations and strategic decision-making with risk management. The Board should have overall responsibility for management of market risks and should decide the risk management policy of the FI and set limits for liquidity, interest rate, exchange rate and equity price risks.

The ALCO is a decision-making unit, consisting of the FI's senior management including CEO, responsible for integrated balance sheet management from risk-return perspective including the strategic management of interest rate and liquidity risks. While each FI will have to decide the role of its ALCO, its powers and responsibilities as also the decisions to be taken by it would normally include:

- Monitoring the market risk levels of the FI by ensuring adherence to the various risk-limits set by the Board;
- Articulating the current interest rate view and a view on future direction of interest rate movements, and base its decisions for future business strategy on this view as also on other parameters considered relevant;
- Deciding the business strategy of the FI, both on the assets and liabilities sides, consistent with the FIs interest rate view, budget and pre-determined risk management objectives. This would, in turn, include:
  - Determining the desired maturity profile and mix of the assets and liabilities;
  - Product pricing for both, assets as well as liabilities side;
- Deciding the funding strategy i.e., the source and mix of liabilities or sale of assets; the proportion of fixed vs. floating rate funds, wholesale vs. retail funds, money market vs. capital market funding, domestic vs. foreign currency funding etc.
- Reviewing the results of and progress in the implementation of the decisions made in the previous meetings.

The ALM support groups consisting of operating staff should be responsible for analyzing, monitoring and reporting the risk profiles to the ALCO. The staff should also prepare forecasts (simulations) reflecting the impact of various possible changes in market conditions on the balance sheet and recommend the action needed to adhere to FI's internal limits.

COMPOSITION OF ALCO

The size (number of members) of ALCO would depend on the size of each institution, business mix and organizational complexity. To ensure commitment of the top management and timely response to market dynamics, the CEO/CMD/DMD or the ED should head the Committee. Though the composition of ALCO could vary across the FIs as per their respective set-up and business profile, it would be useful to have the Chiefs of Investment, Credit, Resources Management or Planning, Funds Management/Treasury (Forex and Domestic), International Business and Economic Research as the members of the Committee. In addition, the Head of the Technology Division should also be an invitee for building up of MIS and related computerization. Some FIs may even have sub-committees and support groups.

COMMITTEE OF DIRECTORS

The Management Committee of the Board or any other Specific Committee constituted by the Board should oversee the implementation of the ALM system and review its functioning periodically.

ALM Process

The scope of ALM function can be described as follows:

- Liquidity risk management
- Management of market risks
- Trading risk management
- Funding and capital planning
- Profit planning and growth projection.

The guidelines contained in this note mainly address Liquidity and Interest Rate risks.

LIQUIDITY RISK MANAGEMENT

Measuring and managing liquidity needs are vital for effective operation of FIs. By assuring an FI's ability to meet its liabilities as they become due, liquidity management can reduce the probability of an adverse situation from developing. The importance of liquidity transcends individual institutions, as liquidity shortfall in one institution can have repercussions on the entire system. FIs management should measure not only the liquidity positions of FIs on an on-going basis but also examine how liquidity requirements are likely to evolve under different assumptions. Experience shows that assets commonly considered to be liquid, such as Government securities and other money market instruments, could also become illiquid when the market and players are unidirectional. Therefore, liquidity has to be tracked through maturity or cash flow mismatches. For measuring and managing net funding requirements, the use of a maturity ladder and calculation of cumulative surplus or deficit of funds at selected maturity dates is adopted as a standard tool.

The Maturity Profile could be used for measuring the future cash flows of FIs in different time buckets. The time buckets, may be distributed as under:

- 1 to 14 days
- 15 to 28 days
- 29 days and up to 3 months
- Over 3 months and up to 6 months
- Over 6 months and up to 1 year
- Over 1 year and up to 3 years
- Over 3 years and up to 5 years
- Over 5 years and up to 7 years
- Over 7 years and up to 10 years
- Over 10 years.

The investments are assumed as illiquid due to lack of depth in the secondary market and are, therefore, generally shown, as per their residual maturity, under respective time buckets. However, some of the FIs may be maintaining securities in the Trading Book, which are kept distinct from other investments made for retaining relationship with customers. Securities held in the Trading Book should be subject to the following preconditions:

- The composition and volume of the Trading Book should be clearly defined;
- Maximum maturity/duration of the trading portfolio should be restricted;

- The holding period of the trading securities should not exceed 90 days;
- Cut-loss limit(s) should be prescribed;
- Product-wise defeasance periods (i.e. the time taken to liquidate the position on the basis of liquidity in the secondary market) should be prescribed;
- Such securities should be marked-to-market on a daily/weekly basis and the revaluation gain/loss should be charged to the profit and loss account; etc.

FIs which maintain such Trading Books consisting of securities that comply with the above standards, are permitted to show the trading securities under 1-14 days, 15-28 days and 29-90 days buckets on the basis of the defeasance periods. The Board/ALCO of the banks should approve the volume, composition, maximum maturity/duration, holding/defeasance period, cut-loss limits, etc., of the Trading Book. FIs, which are better equipped, will have the option of evolving with the approval of the Board/ALCO, an integrated Value-at-Risk (VaR) limit for their entire balance sheet including the "Banking Book" and the "Trading Book", for the rupee as well as foreign currency portfolio. A copy of the approved policy note in this regard, should be forwarded to the Department of Banking Supervision, FID, RBI.

Within each time bucket there could be mismatches depending on cash inflows and outflows. While the mismatches up to one year would be relevant since these provide early warning signals of impending liquidity problems, the main focus should be on the short-term mismatches viz. 1-14 days and 15-28 days. FIs however, are expected to monitor their cumulative mismatches (running total) across all time buckets by establishing internal prudential limits with the approval of the Board/ALCO. The negative gap during 1-14 days and 15-28 days time buckets, in normal course, should not exceed 10 percent and 15 percent respectively, of the cash outflows in each time bucket. If an FI, in view of its current asset-liability profile and the consequential structural mismatches, needs higher tolerance level, it could operate with higher limit sanctioned by its Board/ALCO giving specific reasons on the need for such higher limit. The discretion to allow a higher tolerance level is intended for a temporary period. i.e. till March 31, 2001. While determining the tolerance levels, the FIs may take into account all relevant factors based on their asset-liability base, nature of business, future strategy, etc. The RBI is interested in ensuring that the tolerance levels are determined keeping all necessary factors in view and further refined with experience gained in Liquidity Management.

The Statement of Liquidity may be prepared by placing all cash inflows and outflows in the maturity ladder according to the expected timing of cash flows. A maturing liability will be a cash outflow while a maturing asset will be a cash inflow. It would also be necessary to take into account the rupee inflows and outflows on account of forex operations. Thus, the foreign currency resources raised abroad but swapped into rupees and deployed in rupee assets, would be reflected in the rupee liquidity statement. Some of the FIs have the practice of disbursing rupee loans to their exporter clients but denominating such loans in foreign currency in their books, which are extinguished by the export proceeds. Such foreign currency denominated loans too would be a part of rupee liquidity statement since such loans are created out of rupee resources. As regards the foreign currency loans granted out of foreign currency resources on a back-to-back basis, a currency-wise liquidity statement for each of the foreign currencies in which liabilities and assets have been created, will need to be prepared.

CURRENCY RISK

Floating exchange rate arrangement has brought in its wake pronounced volatility adding a new dimension to the risk profile of FIs' balance sheets. The increased capital flows across free economies following deregulation have contributed to increase in the volume of transactions. Large cross-border flows together with the volatility has rendered the FIs' balance sheets vulnerable to exchange rate movements.

Dealing in different currencies brings opportunities as also risks. If the liabilities in one currency exceed the level of assets in the same currency, then the currency mismatch can add value or erode value depending upon the currency movements. Mismatched currency position, besides exposing the balance sheet to movements in exchange rate, also exposes it to country risk and settlement risk. FIs undertake operations in foreign exchange such as borrowings and making loans in foreign currency, which exposes them to currency or exchange rate risk. The simplest way to avoid currency risk is to ensure that mismatches, if any, are reduced to zero or near zero. However, irrespective of the strategies adopted, it may not be possible to eliminate currency mismatches altogether.

At present, only five FIs (viz. EXIM Bank, ICICI, IDBI, IFCI and IIBI) have been granted restricted authorization to deal in foreign exchange under FERA 1973 by the RBI (ECD) while other FIs are not authorized to deal in foreign exchange. The FIs are, therefore, unlike banks, are not subject to the full rigor of the reporting requirements under Exchange Control regulations. Hence, the MAP and SIR statements prescribed for banks vide AD (MA Series) circular no. 52 dated 27 December, 1997 issued by the RBI (ECD), are not applicable to FIs. In order, however, to capture the liquidity and interest rate risk inherent in the foreign currency portfolio of the FIs, it would be necessary to compile, on an on-going basis, currency-wise Statement of Liquidity and IRS Statement, separately for each of the currencies in which the FIs have an exposure.

INTEREST RATE RISK (IRR)

Interest rate risk is the risk where changes in market interest rates might adversely affect an FI's financial condition. The immediate impact of changes in interest rates is on FI's earnings (i.e. reported profits) by changing its Net Interest Income (NII). A long-term impact of changing interest rates is on FI's Market Value of Equity (MVE) or Net Worth as the economic value of a bank's assets, liabilities and off-balance sheet positions get affected due to variation in market interest rates. The interest rate risk when viewed from these two perspectives is known as earnings perspective and economic value perspective, respectively. The risk from the earnings perspective can be measured as changes in the Net Interest Income (NII) or Net Interest Margin (NIM). There are many analytical techniques for measurement and management of Interest Rate Risk. In the context of poor MIS, and slow pace of computerization in FIs, the traditional Gap Analysis is considered to be a suitable method to measure the Interest Rate Risk in the initial phase of the ALM system. However, the FIs, which are better equipped, would have the option of deploying advanced IRR management techniques with the approval of their Board/ALCO, in addition to the Gap Analysis prescribed under the guidelines. It is the intention of the RBI to move over to modern techniques of Interest Rate Risk measurement like Duration Gap Analysis, Simulation and Value-at-Risk over time when FIs acquire sufficient expertise and sophistication in acquiring and handling MIS.

The Gap or Mismatch risk can be measured by calculating gaps over different time intervals as at a given date. Gap analysis measures mismatches between rate sensitive liabilities and rate sensitive assets (including off-balance sheet positions). An asset or liability is normally classified as rate sensitive if:

- Within the time interval under consideration, there is a cash flow;
- The interest rate resets/reprices contractually during the interval;
- It is contractually pre-payable or withdrawable before the stated maturities;
- It is dependent on the changes in the bank rate made by the RBI.

The Gap Report should be generated by grouping rate sensitive liabilities, assets and off-balance sheet positions into time buckets according to residual maturity or next re-pricing period, whichever is earlier. All investments, advances, deposits, borrowings, purchased funds, etc., that mature/reprice within a specified time frame are interest rate sensitive. Similarly, any principal repayment of loan is also

rate sensitive if the FI expects to receive it within the time horizon. This includes final principal repayment and interim installments. Certain assets and liabilities carry floating rates of interest that vary with a reference rate and hence, these items get repriced at predetermined intervals. Such assets and liabilities are rate sensitive at the time of repricing. While the interest rates on term deposits and bonds are generally fixed during their currency, the interest rates on advances could be repriced any number of occasions, on the predetermined reset/repricing dates and the new rate would normally correspond to the changes in PLR.

The interest rate gaps may be identified in the following time buckets:

- 1 to 28 days
- 29 days and up to 3 months
- Over 3 months and up to 6 months
- Over 6 months and up to 1 year
- Over 1 year and up to 3 years
- Over 3 years and up to 5 years
- Over 5 years and up to 7 years
- Over 7 years and up to 10 years
- Over 10 years
- Non-sensitive.

The various items of rate sensitive assets and liabilities and off-balance sheet items may be classified into various time buckets.

The Gap is the difference between Rate Sensitive Assets (RSA) and Rate Sensitive Liabilities (RSL) for each time bucket. The positive Gap indicates that it has more RSAs than RSLs whereas the negative Gap indicates that it has more RSLs. The Gap reports indicate whether the institution is in a position to benefit from rising interest rates by having a Positive Gap (RSA, RSL) or whether it is in a position to benefit from declining interest rates by a Negative Gap (RSL, RSA). The Gap can, therefore, be used as a measure of interest rate sensitivity.

Each FI should set prudential limits on interest rate gaps in various time buckets with the approval of the Board/ALCO. Such prudential limits should have a relationship with the Total Assets, Earning Assets or Equity. In addition to the interest rate gap limits, the FIs which are better equipped would have the option of setting the prudential limits in terms of Earnings at Risk (EaR) or Net Interest Margin (NIM) based on their views on interest rate movements with the approval of the Board/ALCO.

General

The classification of various components of assets and liabilities into different time buckets for preparing the Gap reports (Liquidity and Interest Rate Sensitivity) is the benchmark. FIs which are better equipped to reasonably estimate the behavioral pattern, embedded options, rolls-in and rolls-out, etc., of various components of assets and liabilities on the basis of past data/empirical studies could classify them in the appropriate time buckets, subject to approval from the ALCO/Board. A copy of the note approved by the ALCO/Board may be sent to the Department of Banking Supervision, Financial Institutions Division.

The impact of embedded options (i.e., the customers exercising their options for premature closure of term deposits, premature encashment of bonds and pre-payment of loans and advances) on the liquidity and interest rate risks profile of FIs and the magnitude of embedded option risk during the periods of volatility in market interest rates, is quite substantial. FIs should therefore evolve suitable mechanism, supported by empirical studies and behavioral analysis, to estimate the future behavior of assets, liabilities and off-balance sheet items to changes in market variables, and estimate the impact of embedded options. In

the absence of adequate historical database, the entire amount payable under the embedded options should be slotted as per the residual period to the earliest exercise date.

A scientifically evolved internal transfer pricing model by assigning values on the basis of current market rates to funds provided and funds used is an important component for effective implementation of ALM system. The transfer price mechanism can enhance the management of margin i.e., lending or credit spread, the funding or liability spread and mismatch spread. It also helps centralizing interest rate risk at one place, which facilitates effective control and management of interest rate risk. A well defined transfer pricing system also provides a rational framework for pricing of assets and liabilities.

The effectiveness of the operational controls mechanism depends upon the right organization structure. A study of the type of hierarchy would serve to highlight this aspect.

ORGANIZATIONAL STRUCTURE

The Hierarchy

The organizational structure of the bank should facilitate an adequate flow of information – upward, downward and across the organization. Typically such a structure from the top would appear as follows:

i. The Board of Directors including the Chairman and Managing Director,

ii. Executive Director,

iii. General Managers (at the Corporate level and Regional level),

iv. Deputy General Managers (at the Corporate level and Regional level),

v. Assistant General Managers (at the Corporate level and Regional level),

vi. Chief Managers, Senior Managers and other junior officers mostly at the branch level.

The structure should be such that it facilitates smooth flow of information flows upward so that the board of directors and the top management is continuously aware of the business risks and the level of operations of the bank. At the same time information that flows down through an organization smoothly facilitates fulfillment of bank's objectives, strategies, and expectations. Further, the policies and procedures are also communicated to field level functionaries. This process is crucial for achieving the ultimate objectives of the bank.

As a part of the process of control mechanism, the board of directors and top management often request presentations and performance reports. Such information enables them to review the bank's progress and assess the performance. Such reviews provide a reflection on the performance of the personnel and also give an indication whether the organization is moving towards the direction of achieving its objectives.

AUDIT AND VIGILANCE

However efficient the systems may be, and however good the top management may be, the importance of Audit and Vigilance cannot be underestimated. In fact, they can be said to form the eyes and ears of the organization. In the banking industry, there is a greater need for continuous monitoring and evaluation of operations. The audit function forms a very important part of the systems that are built in for the banks and calls for periodic review of operations. It seeks to provide an independent assessment of the operations and at the same time verify the level of compliance with the policies and procedures that are in place. To supplement the audit functions in a bank, the vigilance department plays a supplementary role by coming into action to either perform preventive vigilance functions or take disciplinary action against erring staff after reports to that effect are placed before the Vigilance Committee/Chief Vigilance Officer.

An ongoing process of monitoring helps to detect and also correct any deviations immediately. Such activities are – such as the review and approval of journal entries, and management review and approval of exception reports. Other types of monitoring are more or less doing a post-mortem job by detecting deviations after they occur. For the purpose of audit, personnel can be drawn from various sources such as from the branches, administrative offices or even officers with professional qualifications and expertise. The initiative for this purpose should come from the top management who must identify the personnel for such assignments and also decide on the periodicity of monitoring, depending on the level of risk. Normally, such personnel should be reporting directly to the board of directors or its audit committee. In view of the key nature of this job, the personnel should be competent and well-trained with an unbiased approach.

Considering the nature of audit/vigilance functions, it is imperative that this function is distanced from the branch operations and such personnel should have access to verify all the operations conducted in the bank at various levels including the branches and subsidiaries. Further, the audit/vigilance reports should be sent directly to the next higher level of executive who is above the head of the branch/unit that is being audited. This allows for the proper functioning of corporate governance without bias.

Deficiencies or deviations that are identified should be reported immediately to the person(s) concerned. Any exceptional matter should be directly reported to the top management and the board of directors. Apart from such reports, the branch heads should also send their daily, weekly, monthly and quarterly reports to the controlling authorities. All negative observations should be rectified on a timely basis. For this purpose, the audit personnel should also do follow-up exercise. Ultimately, it is the responsibility of the top management to ensure that all discrepancies as pointed out by the auditors are rectified and also to close the relevant file. The board of directors and the top management should periodically receive and review all audit/vigilance reports.

It is essential that all personnel within the bank understand the importance of management control and are actively engaged in the process.

SUMMARY

- This chapter begins with a discussion of Banking Regulation and Supervision. With regard to effective operational control, good housekeeping forms the base. With records in place, the data that is available should be accessible at any time for decision-making. This aspect is covered under the topic: Adequate Information Storage and Retrieval mechanism.
- The norms for control as far as the assets and liabilities are concerned are laid down by the RBI by way of maintenance of CRAR and putting in place the appropriate asset-liability management system, which aspect has been covered in detail. Finally, for the success of any control mechanism, the right organizational structure must be available, which has been explained. Last but not the least, the importance of Audit and Vigilance is as important as eyes and ears to a human body.

Chapter XII

Introduction to Risk Management

After reading this chapter, you will be conversant with:

- What Risk is All About
- Basic Purpose of Risk Management in Banks
- The Process of Risk Management
- Different Types of Risks in Banks
- Overview of Enterprise-wide Risk Management in Banks

RISK

Peter L Bernstein in his celebrated book, 'Against the Gods - The Remarkable Story of Risk', states that, "in the dark ages risk was always associated with God. As the mankind progressed and business and markets grew, the art of risk management grew from primitive stages to the modern day rocket science".

Risk is an inherent component of our life, be it in business or our personal life. The one who is able to manage it properly emerges the winner.

Risks Associated with Business Activities

In simple terms, risk can be defined as any uncertainty about a future event that threatens the organization's ability to accomplish its mission. Business is a trade off between risk and return.

Box 1
There cannot be a business that is risk-free. This is simply because the underlying principle of a "project" implies the effect of current investment, for a future activity, and a future gain after the "project-construction period" is over, which is referred as the "gestation period" or the lead time of the project. Changes in the intervening period can be either positive or negative. When such changes are adverse, say for example, there is time-overrun or cost escalation, the investment in the project results in a net negative value even before the project is completed. Apart from this, there can also be other associated factors such as several unexpected developments both from the internal and external environments that can render the estimated calculations of the project wrong.

Source: ICFAI Research Center.

The word risk may have different meanings to different users. To a lay man, it has connotations that one invariably associates with the games of gambling or reckless behavior in life. In contrast, to an information age company however, taking risk is one of the most important critical success factors as it encourages innovation. Innovations demand trying of new things, and trying something new again calls for uncertainty where one does not know whether one will succeed or fail. Therefore, it is said to be taking a risk. To some others risk or risk-based functioning is a favourite hobby. Those who fall in this category are termed as speculators. Thus, though risk is an inherent feature of life, its level depends upon the person who wants to take it.

One can move forward only by taking risks. Taking no risk at all may make one feel very secure but it means standing still with the inevitable consequence of stagnation in a fast moving business world. Knowledge will grow where people are able to take risks. Failure will also gain knowledge if the reason for failure is known, recorded and passed on to others in the community so that they do not make the same mistakes. Because of this it is vital that failure is acceptable in the community, otherwise people will cover up their mistakes instead of openly analyzing and learning from them. Failure must be seen as a lesson to the community and not as one individuals' problem. Having briefly discussed the overview of what risk is all about, let us now turn our focus towards the definition of risk.

What is Risk?

Recalling our earlier statements, we can say that risk means different things to different people. For some it is "financial" (exchange rate, interest-call money rates), and for others, "an event or commitment which has the potential to generate commercial liability or damage to the brand image". Since risk is accepted in business as a trade off between reward and threat, it does mean that taking risk brings forth benefits as well. In other words, it is necessary to accept risks, if the desire is to reap the anticipated benefits. Risk in its pragmatic definition, therefore, includes both threats that can materialize and opportunities which can be exploited. This definition of risk is very pertinent today as the current business

environment offers both challenges and opportunities to organizations, which have to manage them to their competitive advantage.

Box 2
Time is a dominant factor in risk. Risk and time are the opposite sides of the same coin, for if there were no tomorrow, there would be no risk. Time transforms risk, and the nature of risk is shaped by the time horizon: so future is the playing field. Time matters most when the decisions are irreversible. And yet many irreversible decisions must be made on the basis of incomplete information. Irreversibility dominates the decisions ranging all way from taking the subway instead of a taxi, to building an automobile factory in Brazil, to changing jobs, to declaring war. If we buy a stock today, we can always sell it tomorrow. But what do we do after the croupier at the roulette table cries, "no more bets", or after a poker bet is doubled? There is no going back. Should we refrain from acting in the hope that the passage of time will make luck or the probabilities turn in our favor?

Source: "Against the Gods", Peter L. Bernstein.

Does the Process of "Risk Management" Eliminate risk?

Risk management is a discipline that deals with the possibility that some future event will cause harm. The proper management of risk provides strategies, techniques, and an approach to recognize and confront any threat faced by an organization that seeks to fulfill its mission. The basic concept of Risk management is built on the answers to the following questions:

What can go wrong in the organisation?

What one can possibly do (both to prevent the harm from occurring and in the aftermath of an "incident") in order to avoid or reduce such risk?

If something adverse happens, how will one pay for it?

It is to be always borne in mind that the process of risk management does not aim at risk elimination, but enables the organization to bring its risks to manageable proportions while not severely affecting their income. This balancing act between the risk levels and the levels of profits earned, needs to be well-planned. Apart from bringing the risks to manageable extent, it is also to be ensured that one risk does not get transformed into any other undesirable risk. This transformation takes place due to the inter-linkage present among the various risks. The focal point in managing any risk is to understand the nature of the transaction so as to unbundle the risks that it is exposed to.

In sharp contrast to our country, the discipline of Risk Management is a more popular subject in the western world. This is largely a result of the lessons from major corporate failures, a telling and visible example being the Barings collapse. In addition, there has been the introduction of regulatory requirements that expect organisations to have effective risk management practices. In India, whilst risk management is still in its infancy, there has been considerable debate on the need to introduce comprehensive risk management practices.[1]

Objectives of Risk Management

While discussing the basic objectives of a risk management function, one comes across two schools of thoughts. One speaks about managing risks, maximizing profitability and creating opportunity out of risks and the other concerns with minimizing risks or the loss associated with the business operations and thus protecting corporate assets. The management of an organization needs to consciously decide whether or not it wants to pursue risk management function to 'manage' or 'reduce' risks. Managing risks essentially is about striking the right

1 Shri Kumar Mangalam Birla Committee Report has been instrumental in SEBI amending the listing agreement, which now requires the Audit Committee to review the company's risk management's policies and the Director's to separately report on risks and controls.

balance between risks and controls and taking informed management decisions on opportunities and threats facing an organization. Both these situations, i.e. over or under controlling risks are not desirable as the former means higher costs and the latter means possible exposure to risk.

The process of mitigating or minimising risks, on the other hand, means mitigating or minimizing all risks even if the cost is excessive and outweighs the cost-benefit analysis. Further, it may also mean that the opportunities are not adequately exploited. In the context of the risk management function, identification and management of risk is more prominent in the financial services sector and less so in the consumer products industry.

Approaches to Risk Management

After the different types of risks are identified, the next step involves identifying the alternate approaches available for managing/reducing the risks. The various approaches are described below:

- **Avoidance:** The concept of risk is relevant if the bank is holding an asset/liability which is exposed to risk. Avoidance refers to not holding such an asset/liability as a means of avoiding the risk. Exchange risk can be avoided by not holding assets/liabilities denominated in foreign currencies. Business risk is avoided by not doing the business itself. This method can be adopted more as an exception than as a rule since any business activity necessitates holding of assets and liabilities.

  This approach has application when a bank is planning to decide exposure limits. For example, a bank may decide to avoid a particular industry say, Aquaculture or Poultry, while extending credit or it may decide not to lend to certain type of banks in the money market.

- **Loss Control:** Loss control measures are used in case of the risks which are not avoided. These risks might have been assumed either voluntarily or because they cannot be avoided. The objective of these measures is either to prevent a loss or to reduce the probability of loss. Insurance, for example, is a loss control measure. Introduction of systems and procedures, internal or external audit help in controlling the losses arising out of personnel. Raising funds through floating rate interest bearing instruments can reduce the losses due to interest rate risk.

- **Separation:** The scope for loss by concentrating an asset at a single location can be reduced by distributing it to different locations. Assets which are needed for routine consumption can be placed at multiple locations so that loss in case of any accident can be minimized. However, this does simultaneously increase the number of risk centers. Consider two banks, one which has a wide network across the country and another which is confined to one state. An adverse economic scenario of the state will affect the latter more than the former. This is more conspicuous when one compares a cooperative bank with a commercial bank.

- **Combination:** This reflects the old adage of not putting all the eggs in one basket. The risk of default is less when the financial assets are distributed over a number of issuers instead of locking them with a single issuer. It pays to have multiple suppliers of raw material instead of relying on a sole supplier. A well-diversified company has a lower risk of experiencing a recession.

- **Transfer:** Risk reduction can be achieved by transfer. The transfer can be of three types. In the first type, the risk can be transferred by transferring the asset/liability itself. For instance, the risk emanating by holding a property or a foreign currency security can be eliminated by transferring the same to another. The second type of transfer involves transferring the risk without transferring the asset/liability. The exchange risk involved in holding a

foreign currency asset/liability can be transferred to another by entering into a forward contract/currency swap. Similarly, the interest rate risk can be transferred by entering into an interest rate swap. The third type of transfer involves making a third party pay for the losses without actually transferring the risk. An insurance policy covering the third party risk is an example.

When a bank takes a policy to cover the losses incurred on account of misuse of lost credit cards, it is in effect finding someone to finance the losses while it still has the obligation to pay the Merchant Establishment.

Except for the approach of avoidance, the bank can effectively adopt others since by avoiding risks the bank will not be making any profits. From the above discussion on risk, it is now evident that banks can neither do without profits nor risks. However, mere acceptance of risks to remain profitable does not suffice. Apart from the losses that can be incurred due to the risks, there is also an ultimate danger that the bank itself may fail. The question that arises at this point is what should the bank do in order to take risk for greater returns and at the same time not end up in losses? Risk Management is the solution to such a situation.

RISK MANAGEMENT

At the outset it is to be noted that risk management does not aim at risk reduction. Risk management enables the banks to bring their risk levels to manageable proportions while not severely reducing their income. Thus, risk management enables the bank to take required level of exposures in order to meet its profit targets. This balancing act between the risk levels and profits needs to be well-planned. Risk management basically is a five-step process which involves:

a. Identification of Risks

b. Quantification of Risks

c. Policy Formulation

d. Strategy Formulation

e. Monitoring Risks.

Identification of Risks: Risk can be anything that can hinder the bank from meeting its targeted results. Each risk must be defined precisely in order to facilitate the identification of the same by the banking organizations. This will also enable the banks to have a fundamental understanding of the activities from which risks originate. This understanding will be essential to evaluate aspects related to the magnitude of the risks, the tenor and the implications they have on the accounting aspects. At any point of time, a bank generally will be exposed to a host of risks emanating from the exposures. However, if the bank considers aggregate values of these risks, without considering each risk independently, there may be improper estimation of the risks due to offsetting. To avoid this, all signs of hidden, economic and competitive exposures are to be considered. This is possible when the bank unbundles the risks involved in each transaction. This is in fact the most critical step where most of the time needs to be spent. Unless the bank identifies and understands the nature of the exposures involved in a transaction, it will not be able to manage them. Further, such unbundling also helps the bank in deciding which risks it will have to manage and which it would prefer to eliminate. The process of unbundling also helps a bank in pricing the risk.

Quantification of Risks: By measuring the risks, the bank is indirectly quantifying the consequences of the decisions taken. If risks are not quantified, the bank will neither be aware of the consequences of its decisions nor will it be in a position to manage the risks. Thus, all risks to which the bank is exposed need to be quantified. Quantification of risks is a crucial task and accurate measurement of the same depends extensively on the information available. The quality of

information coming from various branches, however, depends on the reporting system. The information provided needs to be further evaluated to ensure that there is an effective and ongoing flow of information. Technology and MIS play a crucial role here.

Policy Formulation: The next step will be to develop a policy that gives the standard level of exposures that the bank will have to maintain in order to protect cash flows. Policy is a long-term framework to tackle risk and hence the frequency of changes taking place in it is very low. Setting policies for risk management will depend on the bank's objectives and its risk tolerance levels. The risk levels set by the bank should neither be too high that it goes beyond the bank's capacity to manage it nor should it be too low that the profitability is affected. The bank should decide on a particular risk exposure level only if it aids in achieving the bank's objectives and also if it believes that it has the capacity to manage the risk for a gain. If either of the conditions is not met, the bank will have to try and eliminate/minimize the risk.

Strategy Formulation: A strategy is that which is developed to implement a policy. Clearly, a strategy will then be relatively for a shorter period. Given the exposures and volatilities, a strategy helps in managing these risks. Firstly, the possible options and the risks attached to them are examined in order to know the affect of each option on the cash flows and the earnings. With this information, a strategy will be developed to identify the sources of losses/gains and how efficiently the risks can be shifted to enhance profits while reducing the exposure. Strategies differ widely depending on the nature of exposure, the type of transaction, etc. and will also state the instruments that are to be used to manage exposure, tenors and counterparties.

Monitoring Risk: Laying down strategies will not lead to risk management since risk profile cannot be static. Volatile circumstances may change the risk level of the investment and hence require the banks to restore the same to the set target levels. For instance, the bank takes a long position on a loan of US $1 mn. At an exchange rate of Rs.43.50, the risk which the bank is ready to take is up to Rs.0.10 variation. In absolute terms this will be Rs.1 lakh. However, the exchange rate goes down by Rs.0.15 due to which the loss to the bank is Rs.1.5 lakh. This is beyond the target set by the bank. In such circumstances, the bank can take a long position in US$ if it believes that the rate will move up. And in case the rates are expected to go down further, it can either enter into a forward contract or exit from the long position taking up the loss. In either case the bank needs to have a view about the market regarding its future behavior.

Apart from the long-term changes, the exchange rate and the interest rate fluctuations occur on a monthly, fortnightly and even on a daily basis. There should hence be a continuous vigil on the risk profiles. However, the frequency with which the bank can alter strategies or take action to restore these exposure levels to the set targets may not be very high. This is due to the costs that are involved in taking such actions. Considering the above case, to restore the foreign exchange exposure within the set targets, the bank may choose to enter into a forward contract. However, this will involve transaction costs. In such a situation, the bank should decide to go for the transaction only if change in the exchange rate is believed to be long-term. While monitoring of risks should be done on a continuous basis, restoration of the same to the targets should be done after analyzing the extent of fluctuations taking place during a given period and the transaction costs involved in restoring the exposure to the target set. Thus, continuous monitoring helps in eliminating a worst case scenario by identifying those risk levels which have gone beyond the set targets and restoring them to the targeted levels.

While this is the general process for managing any type of risk, by any business firm, for a bank, the risk management process primarily involves Asset-Liability Management (ALM). ALM is discussed elaborately in subsequent chapters.

Box 3

India Risk Management Survey Report 2001 by KPMG

KPMG, one of India's largest professional services organisation

(http://www.in.kpmg.com) undertook the first India Risk Management Survey to establish the profile of risk management practices in India's leading organisations. In addition to becoming a benchmark document in India on risk management, this survey is a part of an initiative by KPMG to conduct national surveys on a variety of topics including business ethics, corporate frauds, information security, etc. The key objective of the survey is to determine the overall level of awareness of the importance of risk management amongst the senior management and their attitude towards the critical Risks faced by them.

Importance of an Effective Risk Management Strategy:

Findings of KPMG Survey

How important is effective risk management strategy for achieving the goals and objectives of your organisation? Most of us are aware of the importance, but only a few venture to think of effecting steps for the mitigation of perceived risks. In the survey referred above, 80% of respondents believed that an effective risk management strategy is important to achieving the goals and objectives of the organisation. None of the respondents indicated that effective risk management is not important at all for their organisation. This indicates that the importance of risk management is well understood and appreciated in today's business environment. However, when we look at how many companies have formal risk management policies, the number is a low 20%. Further, only 37% of respondents have conducted comprehensive risk reviews in their organizations.

Referring further to the above survey, only one in five respondents said that they have a formal risk management policy in their organisation. This is in strong contrast with the riskiness of businesses, where 70% of respondents felt their business is fairly or very risky. The industry most likely to have a formal risk management policy is financial services (45%) and least likely is consumer products industry (12%). While the majority (67%) of respondents says that they perform strategic risk assessment prior to business planning and undertaking major investments, only 27% use risk-adjusted rates of return to assess investments and new projects.

Do you formally apply strategic long-term risk assessment prior to business and investment planning? Do you risk-adjust your required rate of return? Only 37% of respondents said they have carried out a comprehensive review of risks. The frequency, however, varies significantly by industry. 56% of the organisations in electronics/technology and financial services sector have done such reviews, while only 17% in the construction/engineering and 25% in consumer products sector say they have performed a comprehensive risk assessment. This indicates a partial correlation between the perception of riskiness of business and carrying out a risk assessment.

Has your organisation ever carried out an overall, comprehensive review of risks it faces, i.e., do you have a profile of key business risks?

It is surprising to note that almost 40% of the respondents carried out a one-off risk review exercise as against a continuous one. The one-off risk reviews may not prove to be adequate in identifying and managing risks on an ongoing basis in this ever changing and volatile Indian corporate world. Further, just about 40% of the respondents have developed a risk framework for their organisation to categorise different types of risks.

Scope of the Risk Management Function: 79% of respondents state that risk management in their organisation encompasses market, credit, strategic and operational risks. It is encouraging to note that strategic risk is on the agenda of 92% of the respondents. A breakdown of operational risks reveals that more than 70% of respondents are of the view that operational risks include customer, product, organisational, staff, process and physical risks. Customer risk is perceived to be the most important component of operational risk. Perhaps a result of opening up of markets and easing of import restrictions. Winning and retaining a customer is one of the biggest challenges of any business.

Monitoring of Risk

How frequently are you kept informed about risk performance indicators? A key component of risk management is to have an optimal balance between risk and control. However, very few organisations relate the degree of control to the level of risk. In particular, they have not recently considered which resources are being expended on controls in the light of the specific risks and ability to finance them. This may mean that some low-risk areas may be over-controlled, while some high-risk areas may be under-controlled. Has your organisation recently evaluated whether it is over-controlling in the light of your risks and ability to finance them?

Monitoring of risk is viewed as the responsibility of an individual in many organisations. This may be related to the lack of management information on the key performance indicators of risk. Most of the respondents state that monitoring of risk is done as part of periodic management meetings, and also by way of keeping an eye on the competition, updates in technology, change in government policies, movements in markets, foreign exchange rates, etc. Only 49% of the executives receive data on risk, at least on a monthly basis. This means that organisations without real time reporting and a risk-aware culture may be slow to react to changing patterns of risk exposure and loss.

Role of Internal Audit in Risk Management

Internal Audit plays an important role in risk management programmes. While 63% of respondents agree with the statement that it is fairly or very important in risk management, surprisingly, 28% of respondents believe the role of internal audit is largely limited to compliance alone. How important is the role of Internal Audit in your risk management programme? Is the role of Internal Audit mainly…? The Internal Audit profession has undergone a remarkable change over the years with internal audit actively contributing to success of an organisation. The Internal Audit mandate today in leading organisations includes creating risk awareness, developing a risk profile in conjunction with management, devising a strategy to manage the identified risks, etc.

Who is Responsible for Risk Management

88% of respondents say that overall responsibility for risk management is at the senior management level including CEO, CFO, COO and Directors. Though it is the top management who has overall responsibility for risk management, lower and middle management also need to manage risks at their levels. Leading edge organisations across the world are reaping the competitive advantage that arises from a culture where the tone from the top ensures that risk management is a genuine competency of all their people. Most organisations do not have an executive Risk Manager or a Risk Management Committee. For an organisation to manage its risks, it is imperative that the responsibility for risk management should be absolutely clear. Further, there should be tiers or 'lines of defense' to ensure that its entire people are actively managing risks at their levels. SEBI has recently, through incorporation of Clause 49 in the listing agreement, widened the responsibility of Audit Committees to include review of risk management policies.

The survey categorically proves that risk-awareness if felt by all, but very few proceed further to earnestly conduct a complete risk-analysis and to evolve into a sound policy of risk control and risk-management. This may be due to the fact that Indian business and industry have come to grips with the subject quite lately and recently.

Risk Control Measures

Risk management identifies future risks in order to plan control measures to prevent its occurrence, or to control the extent of damage, if it were to occur. Obtaining insurance cover is a generally followed risk covering method against all known and identifiable risks, like loss in transit of goods in domestic trade, political and commercial risks in export business, fire-risks etc. Financial risks are covered by a process known as hedging. Hedging helps to reduce risks associated with market exposure by taking a counter position in the futures market, i.e. buy stock, sell Nifty futures etc. The development of derivatives market is a device for hedging different kinds of financial risks.

Another innovative tool for hedging financial risks is called "Interest-rate-swaps". This is explained as under.

The Corporations in which individual investors place their money have exposure to fluctuations in all kinds of financial prices, as a natural consequence of their operations. Financial prices include foreign exchange rates, interest rates, commodity prices and injustice prices. The changes in the financial prices cause uncertainty in the projected revenues to the corporate sector. And the companies often attribute the cause in decline in incomes to falling commodity prices, raising interest rates, declining home currency value. Necessity is the mother of invention. Human quest to find the solution continues. In this process various financial instruments were invented. Interest rate swap is one of the risk tools that help a corporate to hedge from uncertainties of the interest rate fluctuations.

The Reserve Bank of India has taken a bold step towards rupee derivative trading allowing banks/financial institutions to hedge against interest rate risks through the use of interest rate swaps and forward rate agreements.

Similarly the risk of exchange-rate fluctuations can be covered by entering into forward contract for buying/selling the foreign currency.

Source: ICFAI Research Center.

EMERGENCE OF RISK MANAGEMENT IN BANKS

The banking environment consists of numerous risks that can impinge upon the profitability of the banks. These multiple sources of risk give rise to a range of different issues. In an environment, where the aspect of the quantitative management of risks has become a major banking function, it is of lesser importance to speak of the generic concepts. The different types of risks needs to be carefully defined and such definitions provide a first basis for measuring risks on which the risk management can be implemented.

There have been a number of factors that can be attributed to the stabilisation of the banking environment in the nineties. Prior to that period, the industry was heavily regulated. Commercial banking operations were basically restricted towards collecting resources and lending operations. The regulators were concerned by the safety of the industry and the control of its money creation power. The rules limited the scope of the operations of the various credit institutions and limited their risks as well. It was only during the nineties that banks experienced the first drastic waves of change in the industry. Among the main driving forces that played a crucial role in the changes were the inflating role of the financial markets, deregulation of the banking sector and the increase in competition among the existing and emerging banks.

On the foreign exchange front, the floating exchange rates accelerated the growth of uncertainty. Monetary policies favoring high levels of interest rates and stimulating their volatility emerged. For countries, especially european countries, where intermediation was by far the major channel of financing the economy, disintermediation increased at an accelerated pace. Those changes turned into new opportunities and threats for the players.

These waves of change generated risks. Risks increased because of new competition, product innovations, the shift from commercial banking to capital markets, increased market volatility, and the disappearance of old barriers which limited the scope of operations for the various financial institutions. There was a total and radical change in the banking industry. Here it is worth mentioning that this process has been a continuous one and has taken place in an orderly manner. Thus it is no surprise that risk management emerged strongly at the time of these waves of transformation in the banking sector.

BANKING RISKS

As stated elsewhere, risks are usually defined by the adverse impact on profitability of several distinct sources of uncertainty. Risk measurement requires that both the uncertainty and its potential adverse effect on profitability be addressed. Let us now try to focus on the risk framework purely from the perspective of a banker.

Risk Framework

The variours risks associated with banking may be defined as below and these definitions have the advantage of being readily recognizable to bankers.

i. **Solvency Risk –** Risk of total financial failure of a bank due to its chronic inability to meet obligations.

ii. **Liquidity Risk –** Risk arising out of a bank's inability to meet the repayment requirements.

iii. **Credit Risk –** Risk of loss to the bank as a result of a default by an obligator.

iv. **Interest Rate Risk –** Vulnerability of net interest income, or the present values of a portfolio, to changes in interest rates.

v. **Price Risks –** Risk of loss/gain in the value of assets, liabilities or derivative due to market price changes, notably volatility in exchange rate and share price movements.

vi. **Operating Risks –** Risks arising from out of failures in operations, supporting systems, human error, omissions, design fault, business interruption, frauds, sabotage, natural disaster etc.,

WHAT ABOUT ALL THE OTHERS?

Where do derivatives (swaps, options, futures, etc.) and the *systemic risk* with which they are so closely associated figure? The answer is that derivatives, being exactly that, reflect the risk characteristics of the underlying instruments (i.e., from which they derive), although at times in more complex form. While Derivative risk does not exist in isolation but is found spread across the spectrum of risks associated with derivative contracts, systemic risk is viewed in the liquidity risk context. Some risk management guidelines for derivatives are discussed in detail in later chapters.

The umbrella term 'market/position risk', which bridges some of the interest rate and price risks mentioned above, has found favor as a conceptual counterpoint to credit risk.

Added to these risks are legal risk, regulatory risk, event risk, portfolio concentration risk, behavioral risk, and/or various other risks that can be subsumed within those risks that are mentioned here.

For instance, legal risk seems to forebode trouble as in the UK local authorities, swaps debacle of the early 1990s, where the authorities were found lacking the contractual powers to be legally liable as swaps counterparties. Alternatively, it is equally arguable that to ascertain contractual powers of counterparties is a standard credit risk procedure, that is stressed in any lending manual.

There is a dilemma whether or not to give law and regulation generic risk categories of their own. It is absolutely necessary that documentation needs to be unassailable, that laws and supervisory regulations have to be properly interpreted and complied with, that changes in laws and regulations may expose banks and their customers and the fact that the society we live in is a litigious one. In the light of these, the alternative available is to treat the legal regulatory problems as and when they arise within the risks listed above, with credit risk being the most common field.

Event risk though sounds simple relates to a sudden and unexpected slippage in credit grading suffered either by a bank or when a major counterparty or issuer to whom the bank is exposed. While the former undermines the bank's profitability by raising its interest costs and curtailing its ability to transact certain deals like high grade swaps, the latter could expose the bank to interest rate or price risks.

A common sub-division of operating risks is business event risk. Event risk is too mercurial to be marked as one of the primary banking risks.

Portfolio concentration risk, though not a necessary risk type in its own right, has widespread disciplinary applications and is an integral part of credit risk management. Fraud, error and other human factors like key personnel risk are part of behavioral risk and fall within operating risks.

The other risks cited above do not exist in watertight compartments but can spill over resulting in multiple effects. When there are poor credit risks, a liquidity crises may arise due to a run on deposits. This chain of events was seen in the failure of continental Illinois (1984), Bank of New England (1991) and countless others in the banking history. Also, banks are exposed to price risk losses on failed forward contracts due to defective credit appraisal. Speculation on derivatives can turn an erstwhile creditworthy customer into a bad debtor and also a possible litigant against the bank.

'Pure' and 'Speculative' Risk

A distinction needs to be drawn between the so-called 'pure' (or 'static') risk and 'speculative' (or 'dynamic') risk. These terms are borrowed from the insurance industry, and bankers may find it more helpful to substitute for the former 'one-way risk' (all downside) and for the latter 'two-way risk' (possible upside as well as downside outcomes). In any case, the distinction has been modified by the relatively new concept of expected loss: this makes it possible by definition to do either better or worse than expected, which turns many negative risks into a two-way bet even if the upside is not always 'profit' as we once knew it. Subjecting our banking risks to this revised test, we can tabulate the findings as follows:

i. **Solvency risk –** One-way (downside). Solvency is 'par' and insolvency a disaster.

ii. **Liquidity risk –** One-way. Liquidity is a necessary condition and not a bonus.

iii. **Credit risk –** Hybrid. One-way in the sense that the obligor will not pay more than face value or what is legally due, and may not materialize, in which case you 'win'. Loan trades could also produce winners as well as losers through revaluations. Conversion of hard core debt into shares changes the risk to a price risk, which is two-way.

iv. **Interest rate risk –** Two-way. Risk is both upside and downside.

v. **Price risks –** Two-way. Gains or losses are possible.

vi. **Operating risks –** Mainly one-way, apart from serendipity, the occasional fluke that can yield a windfall gain. Can arguably be classified as two-way in those cases where an expected loss does not materialize (as for credit risk above).

Credit Risk

In simple terms credit risk can be defined as the risk that customers default, or rather fail to comply with their obligation to service the debt. Credit risk can also be stated as the risk of a decline in the credit standing of counterparty. Such a decline in the value of the debt does not connote default, but implies that the probability of default increases. Credit risk is of enormous importance since the default of a small number of important customers can generate large losses, which can lead to insolvency. Credit risk is normally monitored through classical methods in banks. This will be dealt in detail in the later part of the book. The system of limits imposes a ceiling on the amount lent to any customers within a single industry or customers in a given country. The delegation at various levels of the bank also decides, who is responsible for monitoring of credit risks. It is important to note that the various market transactions also generate credit risk. The loss in the event of default depends upon the value of the instruments and their liquidity.

Liquidity Risk

Liquidity risk is considered to be a major risk in the banks. It is the risk of loss arising due to adverse changes in the cash flows of transactions. It can be defined in different ways, such as, extreme illiquidity, the safety cushion provided by the portfolio of liquid assets, or the ability to raise funds at a normal cost.

The extreme illiquidity more often results in bankruptcy of the bank. Thus, it can be said that liquidity risk is a fatal risk. However, it is also to be noted that such extreme conditions are often the outcome of other kinds of risks. For instance, important losses, due to the default of a big customer, can raise liquidity issues and doubts as to the future of the organization. This kind of situation may be sufficient enough to generate massive withdrawals of funds or the closing of credit lines by other institutions which try to protect themselves against a possible default.

Another definition of liquidity risk is that the short-term asset values are not sufficient to match short-term liabilities. From this standpoint, liquidity is the safety cushion which helps to gain time under difficult conditions. Liquidity risk also means having difficulties in raising funds. In such circumstances liquidity risk relates to the inability to raise money at a reasonable cost. The cost of liquidity can increase due to transitory liquidity shortages in the market. Market liquidity has an impact on the cost of funds for all players. The indicators of market liquidity include the volume of transactions, the level of interest rates and their fluctuations, and the difficulties encountered finding counterparty.

Liquidity risk is a normal outcome of standard transactions. These transactions tend to generate a maturity gap between assets and liabilities. Often, banks collects short-term resources and lend long-term. Given this gap between maturities, there exists always a liquidity risk and a cost of liquidity.

Interest Rate Risk

Interest rate risk is defined as the risk of the fall in the earnings due to the movements of interest rates. Most of the balance sheet items of banks generate revenues and there are costs which are attached to the interest rates. Anyone who lends or borrows is subject to interest rate risk. The lender who is earning a variable rate of interest has the risk of experiencing a reduction in his future revenues through a decline in interest rates. On the other hand, the borrower paying a variable rate faces higher costs when interest rate increases. Both these positions are risky since they generate revenues or expend costs indexed to market rates. In some cases, the rate of outstanding loans is directly related to some market rate.

An added source of interest rate risk is embedded in implicit options in banking products. A common example is that of the prepayment of loans which carry a fixed rate. The borrower can always repay the loan and borrow at a new rate, a right that he will exercise when interest rates decline substantially. It is to be also noted that deposits carry options as well, since they can be transferred to term deposits earning revenues when interest rates increase. Optional risks are often called indirect interest rate risks as they do not arise directly from a change in interest rate. On the other hand, they result from the behavior of customers who compare the benefits and the costs of exercising options embedded in banking products, and make a choice depending upon market conditions.

Market Risk

In the simplest terms, market risk can be defined as the risk of adverse deviations of the mark-to-market value of the trading portfolio during the period that is required to liquidate the transactions. Existence of market risk can be for any period of time. Earnings for the market portfolio are the Profits and Losses (P&L) arising from transactions. The assessment of market risk is based on the instability of market parameters: interest rates, stock exchange indexes, exchange rates. The instability is measured by market volatilities. With the help of the volatilities of market parameters and sensitivities of instruments, the changes in market value can be quantified.

The component of market risk can be divided into several dimensions. One dimension is the liquidity risk that forms an important component in all markets where the low volume of transactions makes it difficult to find a counterparty. Another dimension is the presence of volatility risk arising from the fluctuations over time of the instability of the market parameters.

Foreign Exchange Risk

Currency risk arises due to changes in exchange rates. Variations in earnings are caused by the indexation of revenues and charges to exchange rates, or of the values of assets and liabilities denoted in foreign currencies. Foreign exchange risk is one of the major component of market risk. For market transactions, foreign exchange rates form a part of market parameters whose variations are considered together with other market parameters.

A more traditional approach of dealing with foreign exchange risk is to manage risk on a currency-by-currency basis for the banking portfolio. Other techniques that can be used to measure the totality of interest rate risk are dealt in the later chapters.

Solvency Risk

Solvency is the end result of available capital and of all risks taken: credit, interest rate, liquidity, market or operational risks. Thus solvency risk is the risk of being unable to cover losses, generated by all types of risks, with the available capital. Solvency risk can thus be defined as the risk of default of the bank. It is also identical to the credit risk incurred by the counterparties of the bank.

Operational Risk

Operational risks result out of the improper functioning of the information systems, of reporting systems, and of the internal risk monitoring rules. Operational risks are generally observed at two different levels – at the technical level (in cases where the information system, or the risk measures, are deficient) and at the organizational level, (that deals with the reporting and monitoring of risk, and all related rules and policies).

Technical Risks

Technical risks cover a large number of specific risks. Primarily, they include the errors in the recording process of transaction, deficiencies of information system and the absence of adequate tools for measuring risks. Operational risk is of major importance for delivery and settlement. The existence and the importance of such risks are highly dependent on the technical systems used to settle transactions, which have various levels of safety embedded in their designs.

Country Risk

Country risk arises due to cross border transactions that are growing dramatically in the recent years owing to economic liberalization and globalization. It is the possibility that a country will be unable to service or repay debts to foreign lenders in time. It comprises of transfer risk arising on account of the possibility of losses due to restrictions on external remittances; Sovereign Risk associated with lending to government of a sovereign nation or taking government guarantees; Political Risk when political environment or legislative process of country leads to the government taking over the assets of the financial entity (like nationalization, etc.,) and preventing discharge of liabilities in a manner that had been agreed to earlier; Cross border risk arising on account of the borrower being a resident of a country other than the country where the cross border asset is booked; Currency Risk, a possibility that exchange rate change, will alter the expected amount of principal and return on the lending or investment.

In the above backdrop there can be a situation in which seller (exporter) may deliver the goods, but may not be paid or the buyer (importer) might have paid the money in advance but was not delivered the goods for one or the other reasons. As per the RBI guidance note on Country Risk Management published recently, banks should reckon both fund and non-fund exposures from their domestic as well as foreign branches, if any, while identifying, measuring, monitoring and controlling country risk. It advocates that banks should also take into account indirect country risk exposure. For example, exposures to a domestic commercial borrower with large economic dependence on a certain country may be considered as subject to indirect country risk. The exposures should be computed on a net basis, i.e., gross exposure minus collaterals, guarantees etc. Netting may be considered for collateral guarantees issued by countries with a lower risk and may be permitted for the banks dues payable to such countries.

RBI expects banks to eventually put in place appropriate systems to move over to internal assessment of country risk within a prescribed time frame. The system should be able to identify the full dimensions of country risk as well as incorporate features that acknowledge the links between credit and market risks. Banks should not rely solely on rating agencies or other external sources as their only country risk-monitoring tool. Banks are also advised by RBI to set country exposure limits and monitor such exposure on weekly basis before eventually switching over to real time monitoring. They are also expected to disclose the “Country Risk Management” policies in their Annual Report by way of notes.

Environmental Risk

As the years roll by and technological advancement continues, expectation of the customers change and enlarge. With the economic liberalization and globalization, an increasing number of national and international players are operating in the financial markets, particularly in the banking field. This provides the platform for environmental change and exposes the bank to the environmental risk. Thus, unless the banks improve their delivery channels, reach customers, innovate their products that are service oriented, they are exposed to the environmental risk resulting in loss in business share with the consequential impact on profits.

Contingency Risk

The off-balance sheet items such as guarantees, letters of credit, underwriting commitments, etc., will give rise to the contingency risk. One important feature of the various risks of the banks is that there is a definite linkage between them. For example, if the bank charges its client a floating rate interest, in situations of increasing interest rate scenario, the bank’s interest rate risk will be lower. This enhances the payment obligation of the borrower. Other things remaining constant, the default risk increases. If the client is not able to bear the burden of the rising rates, there may be a possibility of default. Thus, there may be instances where the interest rate risk may eventually lead to a credit risk. Further, the credit risk itself is closely associated with the forex risk in case of the borrowers whose earnings are extremely influenced by exchange rates.

Enterprise-wide Strategic Risk Management

When speaking of the risk management process, it is essential to take a holistic view. This can be done when one views risk management from the framework of "Enterprise-wide Strategic Risk Management".

In today's world, the most advanced companies are evaluating and quantifying their risk and performance on an enterprise-wide basis. They do this not only in order to best control their losses and manage risk on a firm-wide basis, but also to create a competitive advantage in the market place. They integrate enterprise-wide risk management into both their strategy and their culture. Enterprise-wide strategic risk management is a multi-staged process that begins with the quantification and timely reporting of the total risk in the overall firm. This includes quantification of market (including currency and interest rate), credit, liquidity, and operational risks. Limitations on the amount and type of risk carried by the firm are then established and are a function of the capital available to the firm and the firm's strategic goals. These are typically expressed as Value at Risk, Earnings at Risk, or Profit at Risk limits.

The risks in the overall firm are then adjusted to bring them in tune with the parameters or limits defined by the firm's strategic goals. This is followed by monitoring the risk in the firm, which is then quantified, and corrected on a daily or weekly basis to ensure that the risk profile of the firm remains aligned with the strategic vision of the firm.

Regular risk-adjusted performance evaluations ensure that the risk capital allocated to each business is earning the minimum targeted risk-adjusted returns. If not, it should be reallocated to areas where it can earn higher risk-adjusted returns.

This process ensures providing timely, accurate, and comparable quantitative, enterprise-wide risk information to the senior management, enabling ultimately rapid risk management decisions to be made and facilitating the mitigation of losses that can be minimized.

The above mentioned steps aid in the allocation of scarce and expensive capital to vital areas of the firm that produce the highest risk-adjusted returns over the long-term. This enhances shareholder value, smoothes earnings volatility, and can lower the firm's cost of capital thereby creating a competitive advantage.

Till now we have surveyed the basic sources of risk encountered in the banking business. Problems related to credit, liquidity, and fraud are the most common primary causes of bank failures, and combinations of these misfortunes are often evident. Capital inadequacy for the risks being run is an almost universal secondary cause, and prelude to banking insolvency. The above risks are highlighted, but in truth any of the other categories of banking risks discussed are themselves capable of precipitating a collapse; otherwise they would not merit a place on the generic list.

The next chapters will examine each of these risk categories in turn, suggesting how to monitor and manage them in the light of professional experience and scientific analysis. The aim always must be to optimize the risk/reward relationship, avoid shocks (from excessive exposure to particular sources of risk), and provide a prudent cover for expected and unexpected loss. Getting this right is the key to survival and consistent success of a banking entity.

SUMMARY

- The word risk may have different meanings as per the user. For some it is "financial" and for someone else "an event or commitment to generate brand image". In the dark ages risk was associated with God. Risk is inherent component of life whether it is in Business or in the personal life.
- Risk can be defined as any uncertainty about a future event that threatens the organization's ability to accomplish its mission. No business exists without risks or has zero risk-orientation. Risk management cannot be eliminated but enables the organizations to bring it to manageable proportions. Risk management basically is a five-step process, involving (i) Avoidance, (ii) Loss control, (iii) Separation, (iv) Combination and (v) Transfer. One can move forward only by taking risks. Knowledge will grow where people are able to take risks.
- The management of an organization has to decide whether they want to pursue their risk management function in order to 'manage' or 'reduce' risks. In the context of the risk management function, identification and management of risk is more prominent for the financial services sector and less so for consumer products industry. Solvency and liquidity are the two irreducible conditions upon which society allows the banking industry to gear up. Problems with credit, liquidity, and fraud are the most common primary causes of bank failures, and combinations of these misfortunes are often seen.

Chapter XIII

The New Basel Accord – Implication for Banks

After reading this chapter, you will be conversant with:

- An Overview
- Basel II Framework – The Three Pillar Architecture
- Organizations Affected by Basel II
- Impact of Basel II

Effective risk management strategies can be implemented by integrating effective bank-level management, operational supervision and market discipline. It is also imperative for financial institutions to update their risk management practices in accordance with prevalent legislation and regulatory environment. With these aspects in mind, the Basel Committee on Banking Supervision published the Capital Adequacy Accord, also known as the Basel Accord, in 1988. The Basel Accord defined the parameters of risk management and capital adequacy for Financial Service Providers (FSPs). With the growth in the financial services sector, the Committee felt the need to update the Accord in line with new developments. As a result, it proposed the New Basel Capital Accord, also known as Basel II, in June 1999. With its new risk-sensitive framework, Basel II aims to fill the gaps left by the previous Accord. Basel II was devised to improve the soundness of the financial system by aligning regulatory capital requirement to the underlying risks of the banking industry. It encourages banks to conduct better risk management and enhance market discipline. According to the Committee, financial institutions should integrate Basel II in their operations by the year-end 2006. Efficient risk management, as outlined by Basel II, can be ensured by leveraging information technology. A more coherent architecture, would be required for process automation and integration, and cost reduction mechanisms. The chapter discusses Basel II, its framework and its impact on financial organizations.

AN OVERVIEW

Financial markets have always been sensitive towards incurring heavy losses due to either poor risk management policies or frauds – as both would reduce public confidence, which is the mainstay of the sector. Thus, banking institutions and investment firms felt the need to improve their measures for security and risk management. To achieve this, the Basel Accord was signed in 1988.

The Basel Accord was adopted by the Central Banks of over 100 countries as a basis of risk management within their banking system. It aimed to ensure an adequate level of capital in the international banking system. However, the regulatory capital requirement set by the Accord proved to be incompatible with the new sophisticated internal measures of economic capital. In addition, the Accord was unable to recognize credit risk techniques, such as collateral and guarantees. This resulted in an inflexible system and ultimately increased the risk for financial institutions. Basel II was devised to plug these gaps. A Basel II implementation allows bankers to adequately emphasize their own internal risk management methodologies. Bankers can also provide more incentives and options for risk management, thereby increasing flexibility of their systems. In addition to this, Basel II provides a variety of benefits to the banking system. These include enhanced risk management, efficient operations, and higher revenues to the banking community.

Along with the increased benefits, Basel II has also laid down some controls on the international banking system. This is primarily in the form of a higher capital requirement to underwrite mismanagement of risks and lack of infrastructural controls in many economies. The global acceptance for Basel II is not far and most banks across the world will soon come under the purview of this Accord.

Comparing the new Accord with the existing one.

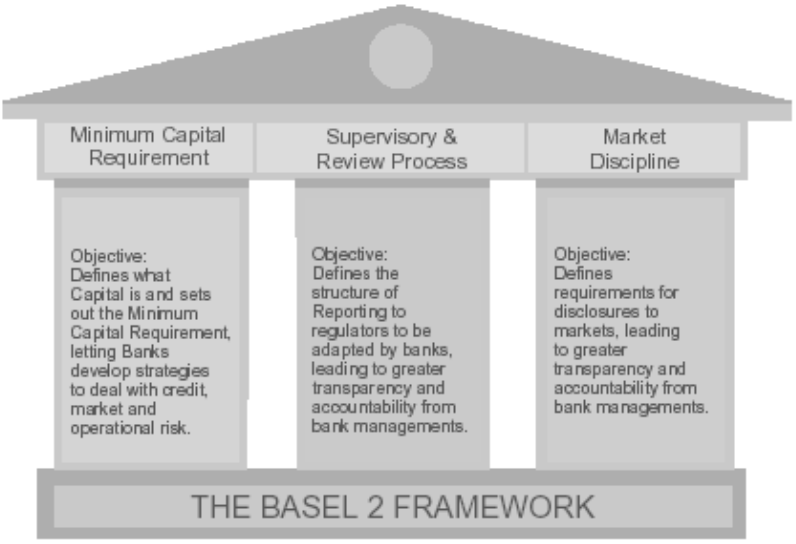
Existing Accord	New Accord
1. Focus on single risk.	1. More emphasis on banks' measures – own internal methodology, supervisory review and market discipline.
2. One size fits all.	2. Flexibility, menu of approaches, incentive for better risk management.
3. Broad brush structure.	3. More risk sensitivity.

After a series of revisions, Basel II has been finalized. A major part of it will be applicable by the end of 2006. During this intervening period, banks and supervisors must develop the necessary systems and processes to comply with the standards laid down by Basel II. For instance, financial institutions have to maintain a history of vital data sets built prior to the implementation date of Basel II. This will help them seamlessly "migrate" to Basel II. In addition, many countries have already started work on draft rules that would integrate Basel capital standards with their national capital regimes. The Basel II Accord aims to ensure effective risk management and security systems in the financial sector. It has undergone rigorous revisions before its framework has been finally frozen for implementation.

THE BASEL II FRAMEWORK

Basel II intends to provide more risk-sensitive approaches while maintaining the overall level of regulatory capital within the financial system. This can be achieved through its meticulously designed framework that consists of three mutually reinforcing pillars as summarized in Figure 1.

Figure 1: The Three Pillar Architecture as defined by Basel II



Source: ICFAI Research Center.

PILLAR 1

Minimum Capital Requirements

The first pillar is designed to help cover risks within a financial institution. It aims to set minimum capital requirements and defines the current amount of capital. This pillar also stresses on defining the capital amount by quantifying risks such as Credit Risk, Operational Risk and Market Risk.

MEASURING CREDIT RISK

Credit Risk defines the minimum capital required to cover exposure to customers and counter parties. The Basel II framework provides a menu of approaches in respect of credit risk. They are:

i. Standardized Approach,

ii. Internal Rating Based (IRB) Approach
   a. Foundation
   b. Advanced.

i. **Standardized Approach:** In this approach, the bank allocates a risk-weight to each of its assets and off-balance sheet positions. It then calculates a sum of risk-weighted asset values. A risk weight of 100% indicates that an exposure is included in calculation of assets at full value. The capital charge is equal to 8% of the asset value. This approach, while remaining essentially the same as in the earlier Accord, however, includes a higher sensitivity to risk. As per the earlier Accord, individual risk weights were dependent on the category of borrowers such as sovereign nations or banks. In Basel II however, these weights can be defined by referring to a rating provided by an external credit assessment agency.

ii. **Internal Ratings Based Approach (IRB):** In this approach, banks use their internal evaluation systems to assess a borrower's credit risk. The results, attained by this process, are translated into estimates of a potential future loss, thereby defining the basis of minimum capital requirements.

The IRB Approach supports the following methodologies for corporate, sovereign and bank exposures:

Foundation – Using this methodology, banks can estimate the risk of default or the Probability of Default (PD) associated with each borrower. Additional risk factors such as Loss Given Default (LGD) and Exposure at Default (EAD) are standardized by supervisory rules that are laid down and monitored by regulating authorities.

Advanced – This methodology allows banks with sufficient internal capital to assess additional risk factors. These factors include Exposure at Default (EAD), Loss Given Default (LGD) and Maturity (M). It also allows banks to provide guarantees and credit derivatives on the risk of exposure. The ranges of risks in both these methodologies are more diverse than in the standardized approach, resulting in greater risk sensitivity.

Credit Risk Mitigation

The Consultative Document contains proposals for the recognition of certain credit risk mitigation techniques in the calculation of regulatory capital. These include collateral, guarantees and credit derivatives and on-balance sheet netting. Certain minimum conditions must be met in each case to qualify for relief of capital.

- In the case of collateral, these include legal certainty, low correlation with exposure and the operation of robust risk management practices.
- Similar requirements apply to on-balance sheet netting. For guarantees and credit derivatives a range of operational requirements are specified.

Asset Securitization

The Committee has put forward proposals that are designed to look through traditional asset securitisation structures to ensure that a capital charge is levied in respect of risks retained by the bank. Proposals are aimed at the level of originating, investing and sponsoring banks. Originating banks qualify for a relief from the capital charge only where it is established that the securitised assets have been effectively removed from the balance sheet. Any credit enhancements provided are deducted from the originating banks' regulatory capital.

Investing banks carry a capital charge based on the credit rating of the assets they hold, where they are using the standardised approach for credit risk. If they adopt the internal ratings based approach, the capital charge will be determined by their internal estimates of PD, etc.

Sponsoring banks must also deduct credit enhancements provided to securitisation structures from regulatory capital. Pure liquidity facilities provided by originators or sponsors are regarded as commitments for regulatory purposes. The Committee has proposed detailed operational rules to ensure that implicit credit protection is not being provided by originating or sponsoring banks through these liquidity facilities.

MEASURING OPERATIONAL RISK

In Basel II, the operational risk can be measured using the following three approaches:

1. **Basic Indicator Approach** - This is a traditional approach, which links the capital charge for operational risk to a single operational parameter, such as the bank's gross annual revenue. The capital charge is calculated as a fixed percentage of this parameter, defined as the 'Alpha Factor'.
2. **Standardized Approach** - This approach is a variant of the Basic Indicator Approach. Here, the activities of a bank are divided into standard industry business lines, such as corporate banking, trade finance and many more. These business lines are then mapped by banks into their internal framework. A percentage of capital charge, known as the 'Beta Factor', is defined for each business line. The bank can calculate its capital charge for a business line by applying the Beta Factor to the indicator value for the business line. The total capital charge for the bank is calculated as the sum total of all capital charges for individual business lines.
3. **Internal Measurement Approach (IM)** - This is the most sophisticated of all the approaches. Here, risk is measured using the bank's internal loss data. Typically, a bank collects data inputs for a specified set of business lines and risk types. These inputs include an operational risk indicator, data indicating the probability of a loss event, and the losses incurred in case these events take place.

MEASURING MARKET RISKS

Market Risk determines the capital required to cover exposure to changes in market conditions - such as fluctuations in interest rates, foreign exchange rates, equity prices, and commodity prices. The approaches to determine market risk are the same as those defined in the earlier Accord.

Benefits of the First Pillar

The first pillar aims to refine the measurement the framework set out in the 1988 Accord by effectively reducing risk across the banking system. Different reporting systems, which comply with objectives set by this pillar, will help track and report risks as they occur, thus eliminating them at the outset. It will allow banks to set-up independent audit functions to scrutinize the possibilities of risks. The minimum capital requirement is expected to reduce considerably for banks and other financial institutions. Furthermore, banks will support a complete alignment of regulatory, book and economic capital.

PILLAR 2

Supervisory and Review Process

The second pillar of Basel II intends to ensure the presence of sound processes at each bank. This pillar would also provide the framework to assess the adequacy of the bank's capital, based on a thorough evaluation of its risks. The Basel II framework emphasizes the development of an internal capital assessment process by the bank management. Additionally, management should set targets for capital corresponding with the bank's risk profile and control environment.

Regulatory and supervisory bodies (either the Central Banks or bodies setup by the Central Bank or Government, for regulation and control) will review the internal process. This is done so that an assessment of the bank's capital adequacy in relation to its risks can be made. A point to note is that compliance with internal measurement methodologies, mitigation policies of credit risk, and securitization policies for minimum qualifying standards are subject to supervisory control. The supervising authority will also be responsible for reviewing operations and processes in trading, Internet Banking and Security Processing.

Benefits of the Second Pillar

The implementation of the second pillar demands increased interaction between bank managers and supervisory bodies. This increased level of interaction enhances the level of transparency within the organization. The second pillar helps achieve a higher level of security within the organization. A level of standardization and conformity is established across the enterprise. This in turn would help achieve higher returns with lower risk.

PILLAR 3

Market Discipline

The third pillar of the new framework attempts to boost market discipline through enhanced disclosure by banks. Basel II identifies the disclosure requirements and provides recommendations both on the defining methods for calculating capital adequacy, and risk management strategies. Effective disclosures by banks help market participants understand the bank's risk profile and adequacy of its capital positions, thereby facilitating market discipline. This strategy plays an important role in maintaining the confidence in a financial institution.

A guidance paper presented in January 2000 has six broad recommendations related to capital, risk exposure and capital adequacy. Based on these recommendations, the committee has laid down more specific quantitative and qualitative disclosures in key areas. These include the scope of application, composition of capital, risk exposure assessment and management processes, and capital adequacy. In general, it provides enhanced disclosures on risk and capital adequacy.

Benefits of the Third Pillar

The third pillar of the Basel II framework helps to increase awareness of all the risks in the banking sector through a process of detailed disclosure. It also helps align economic capital data to book and risk capital data. Further, this pillar reveals the annual losses incurred by business lines and asset classes. This helps increase transparency.

Organizations affected by Basel II

All banks and financial institutions in the G10 countries intend to incorporate the Basel II Accord through local regulators. A high possibility of the earlier accord being replaced by Basel II in the other countries also exists. The European Union is the first adopter of this accord, and the recommendations of this accord are being integrated into a new EU directive. In addition, the European Commission intends to apply this accord to all investments, businesses and credit institutions. The accord's adoption in other continents like Australia, Asia and in North and South America would be phased. It would primarily depend on proposals submitted by the regulatory authorities on implementation of the accord. The accord's scope of application will include banks and enterprises involved in securitization and with long-term equity holdings such as private equity and venture capital. It will also apply to all the parent and subsidiary companies of banking groups.

Basel II will be applicable to organizations offering the following financial services:

- Corporate Finance,
- Retail Banking,
- Asset Management,
- Trading and Sales,
- Payments and Settlements,
- Commercial Banking,

- Retail Brokerage,
- Agency and Custodial Services.

Basel II will facilitate data and system integration across banking groups.

Box 1
Based on the consensus reached on May 11, 2004 the Basel Committee was expected to publish the final Basel II Accord by the end of June 2004. The committee aims to implement Basel II for the standardized approach (using external ratings for calculating risk weights) and the foundation approach (using banks' internal ratings for calculating probabilities of default and related risk weights) by the end of 2006. For the advanced approach – using banks' internal ratings for calculating both probabilities of default and loss given default and related risk weights – the envisaged date of implementation is by the end of 2007.

Source: Are Basel II's pillars strong enough? Harald Benink.

THE IMPACT AND CHALLENGES OF BASEL II

Major banks and financial institutions in Europe and the United States have already started incorporating Basel II as part of their systems. The impact on the G-10 countries, where the accord is still being analyzed, will lead to a further regulation of banks, insurance and investment agencies. Japan, along with many developing economies may be affected due to a lack of transparency in its banking sector The New accord will significantly affect a wide range of organizations.

Operational Impact

Basel II will affect different spheres of financial activities. Therefore, its impact can be based on different kinds of operations conducted by organizations. These may include:

Rating Agencies

All Rating Agencies will incorporate the New Accord in their operational systems to evaluate banks globally. They intend to do this by using the advanced measurement approach with third-party evaluations. Incorporating this accord will result in establishing a more competitive and safer banking system.

Financial Industry

Basel II primarily applies to banks, but most legal rulings have emphasized on the harmonization of rules across all financial sectors. Many financial institutions that provide services such as credit cards and equities will also come under its purview.

Basel II will also have a major impact on the insurance sector, as it will allocate and account for risk capital and enterprise-wide risk management. The transparency achieved by Basel II for risk management and capital reserves will fundamentally change the reinsurance business.

It will also affect the securitization of risk. The impact of Basel II will extend to the state owned and managed financial institutions. These institutions will be required to meet market requirements for capital efficiency and optimization. In addition, banks in developing markets will need to invest capital for upgrading their infrastructure. When implemented, Basel II will lead to a restructuring of costs and prices for all financial services.

Finally, the introduction of operational risk in Basel II could affect the capital charge of banks. It would increase unless the bank adopts the more sophisticated approaches for measuring credit and operational risks.

Assessment of the Proposals

The Basel II proposals are assessed on two levels:

a. An operational assessment and

b. Strategic assessment – the longer-term strategic implications for banking and risk management.

Operational Assessment

The second Consultative Document marks a significant change in the thinking of the Basel Committee. In the area of credit risk it has responded to the negative reaction to the proposed role for the rating agencies in determining capital requirements. The Internal Ratings Based approaches (IRB) are significant steps in aligning regulatory capital estimation with evolving best practice in credit risk management. Much work remains to be done to sort out the calibration and the operational requirements. However, when finalised, this will provide the basis for ensuring that banks will be rewarded for having sound capital allocation practices that are based on advanced risk management tools. In this sense, the proposals should achieve the objective of enhancing banking soundness insofar as this can be achieved through capital management.

However, the operational risk proposals are not ready for implementation to the satisfaction of the industry. Much of the detail has yet to be worked out. It is unlikely that the calibration of risk factors will be concluded in time for finalisation of the New Accord. Most banks have yet to begin to build loss data from which they may determine loss probabilities. Many of the factors driving operational risk are organisation specific. It is more logical to manage the risk through the supervisory review process in Pillar 2. This is the approach adopted for interest rate risk in the banking book, which was included in the first consultative document under minimum capital requirements but was moved, following the consultation process, into Pillar 2.

The approach adopted for interest rate risk is to set out a series of best practice principles on the management and supervision of this risk. This framework has the benefit of facilitating the evolution of best practice over time and could easily be extended to operational risk.

The Pillar 1 incentive structures further need considerable work. Operational requirements for internal measurement of credit and operational risks require validation of the risk assessment processes based on stringent data requirements. For example, banks are allowed to use their internal ratings for credit risk purposes if they are based on data collected over an extended period that would include a complete business cycle. The minimum observation period over which banks are required to hold the necessary data is five years.

STRATEGIC ASSESSMENT

An assessment of the strategic implications is complicated by the fact that so much depends on the final shape and detail of the New Accord. The proposals on credit risk, if suitably modified during the consultation process, should bring about an improved alignment between regulatory and economic measures of the capital. This will enable and encourage banks to exercise a sharper focus on shareholder value without the distortions from an outdated regulatory capital regime.

However, decisions on the treatment of operational risk could adversely impact on the objective of aligning economic and regulatory measures of capital. The quantum of capital proposed for operational risk is substantial. In addition, there is potential for conflict between the objectives of developing risk sensitive regulatory capital measures for operational risk and the Basel Committee's aim to maintain at least the same overall level of capital as is currently maintained by the banking system.

The banking industry acknowledges that quantification of operational risk in a consistent manner is still at an early stage. The adoption of an over simplistic measure, without due recognition of specific risks and risk management processes could prejudice the integrity of the proposed new regulatory regime.

SUMMARY

- Effective risk management strategies can be implemented by integrating effective bank-level management, operational supervision and market discipline.
- The first pillar of Basel II is designed to help cover risks within the financial institutions.
- The second pillar of Basel II intends to ensure the presence of sound processes at each bank.
- The third pillar of Basel II attempts to boost market discipline through enhanced disclosure by banks.
- The consultative document contains proposals for the recognition of certain credit risk investigation techniques in the calculation of regulatory capital.

Chapter XIV

Operational Risk Management

After reading this chapter, you will be conversant with:

- Operational Risk and its Evolution
- Major Sources of Operational Risk
- Measurement of Operational Risk
- Management of Operational Risk

The banking environment is continuously changing. The comfort of an insulated environment offered by regulations in the past is vanishing. The resulting uncertainties give rise to risks, and make it imperative to call for risk identification, measurement and management. One such all-pervasive risk that banks face is operational risk. It is one of the oldest risks in banking that has been managed all along quite informally but of late has suddenly caught everybody's attention. This increased attention could be owing to the expansion in the range of activities being pursued in the recent past, perceived increase in operational risk itself, reaction to major loss events that have occurred internally, threat of increased competition by virtue of blurring boundaries among financial services providers, information technology initiatives and the resulting falling spreads, management commitment for enterprise-wide risk management, regulatory attention, etc.,

Sound operational risk management is essential to counter any real operational risk of a financial institution in order to promote stability in the financial system as a whole. Risk management is often defined as hedging or neutralizing the financial risk that results from a series of transactions. Effective operational risk management is the mixture of policies, procedures, expertise and systems that the institution needs to manage all the risks associated with banking business. It includes matters such as inappropriate organizational structure, unavailability of systems, business failures, defective controls, fraud, and human error. Further modification of operational procedures and controls are necessary as risk management becomes more challenging in a fast paced market. Recent market occurrences have also created a particularly strong sentiment for establishing an effective risk management practice.

Failure to adequately manage operational risk can negatively impact profit/loss, not only resulting from the costs of incorrect settlement of transactions but also from managing incorrect positions or taking unknown credit risk. It is essential to know that the basic risk management practices are the division of duties between operational personnel and trading personnel. They have been responsible for confirmation and for settlement and must maintain a reporting line independent of trading where the trading takes place. The financial industry has been recently reminded of this very essential control first with Barings and again with Daiwa Bank. Both these incidents have prompted the organizations to focus on traders and market practices as well as on operational control.

Operational controls are important to risk management process. Effective controls help the banks to detect and identify problems before incurring financial loss. Many organizations and institutions started responding to this risk by implementing tighter controls within their operations. However, managing operational risk encompasses managing business processes, human technology and capital.

Traditionally, the concept of risk from financial markets has focused on financial risks and derivative products. Despite this fact, the industry has generally allocated few resources and limited attention to the active management of operational risk. Within the financial markets, risk management focuses too often on the market and the credit risk. A fully integrated approach to risk management involves determining the company's risk appetite and setting up of the risk agenda. This tends to give more support to the management that is proactive. A comprehensive approach to risk management covers three key aspects of business organization – its strategy, its processes and its people. By adopting this, companies as well as organizations can improve the profitability of their businesses, either by removing the cost of existing control tasks, or by taking more risk.

OPERATIONAL RISK AND ITS EVOLUTION

Though operational risk is as old as banking, preceding even market and credit risk, its definition is still evolving with no unanimously agreed-upon, universal definition. Operational risk is often defined by what it is not: Any risk that is not related to credit, market and liquidity risks. Different banks perceive it in different ways as could be gauged from the following (Operational Risk: the next frontier, 1999):

- Any risk not categorized as market or credit risk;
- A risk of loss arising from various types of human or technical error;
- Risk associated with settlement or payment risk and business interruption and legal risk;
- Risk of frauds by employees and outsiders; unauthorized transactions by employees and errors relating to computer and telecommunication systems;
- The potential exposure to missed opportunity or to unexpected financial, reputational, or other damage resulting from the way in which an organization operates and pursues its business objectives;
- Risk arising from inadequate systems, operational problems, breaches in internal controls, fraud, and unforeseen catastrophes resulting in unexpected losses for the organization. Essentially, operational risk is present in every aspect of the business processe undertaken by the organization and in the systems, procedures, and personnel employed to administer those processes.

The definitions of Operational Risk traditionally focus on the risk associated with operations/transactions processing. Many banks perceive processing risk is of primary importance with the highest potential magnitude of consequences. Some banks do not agree to classify settlement, collateral and netting risk under operational risks. Some banks treat technology risk as operational risk, while some view it as a separate risk category. But all banks see some form of link between market, credit and operational risk.

Some banks consider business risk as the second most important risk and hence prefer to include it under operational risk. Some, however, argue that as business risk is imparted more by market volatility, it should be included in market risk. Yet others are preferring to treat it as a separate risk such as credit and market risk. In this context, one needs to appreciate the fact that it is the business strategy which, normally indicates the business domain and the products and services to be offered; differential advantage sought in terms of quality, price, service, and the basis on which these are to be achieved; strategic thrusts through selected programs and their timing and the goals. Secondly, it defines the overall desired portfolio of a bank and major moves regarding retention, addition or deletion of business segments, consolidated resource mobilization and plans. Thirdly, if we accept the definition of operational risk as “everything but market and credit risk”, business risk gets automatically included under the umbrella of the operational risk. Viewed against this perspective, there appears to be a case for inclusion of business/strategy risk under operational risk.

The Basel Committee on Banking Supervision defined Operational Risk as, “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”. A similar expression echoes from the definition given by PricewaterhouseCooper based on its survey of a few global banks: “Operational risk is the risk of direct or indirect losses resulting from inadequate or failed internal processes, people and systems or from external events”. These definitions have indeed captured the whole horizon of operational risk except for “business-strategic risk”, though it is equally critical.

Many industry leaders consider "human behavioral risk" as the most challenging aspect of operational risk. Many of the operational risk-related functions such as regulatory compliance, finance management, frauds, IT, legal, and insurance are carried out by the employees (Blunden, AC and Hill VJH 2000).

Operational risk is perceived to be highly capable of impacting business lines that have high volume and high turnover coupled with low-margins. The Survey of Operational Risk carried-out by PricewaterhouseCoopers in 1997 in conjunction with the British Bankers' Association in the banking industry revealed that high levels of loss occurred in the categories of system failures, criminal acts, legal action, erroneous funds transfer, business interruption costs and damage to assets. The survey also revealed that –

- An average of 30% of respondents in banks do not evaluate the impact of operational risk;
- Of those that do, 44% use risk-ranking techniques;
- Only a few use more sophisticated risk models to estimate the impact and probability of risks; and
- The rest use a variety of other undefined methods.

The results of the survey also suggest that fresh research is needed in the areas of:

- Rigorous evaluation and measurement of operational risk;
- Education and awareness of Board of Directors on an enterprise-wide basis;
- Providing the required information to the management and Board of Directors to enable them to make timely and well-founded decisions; and
- Framing formal policies, definitions and approaches.

In view of the complexity of operational risk, it is essential for any bank to define operational risk in its own terms as understood in the context of its organization and particularly communicate the same to the staff members for, without a fair understanding of the organization's philosophy of risk management, no effective implementation could be possible.

Managing Operational risk

Financial institutions need to adopt integrated, proactive programs for managing operational risk in order to avoid the recurring operating losses, to face the growing complexity of the trading environment and to meet the client demand.

Without proper management of operational risk, an organization cannot control its market and credit risk exposure. To do this effectively, it is necessary to have the relevant skills in various fields and knowledgeable staff, technical and good infrastructural facilities as well as control systems.

Measuring Operational Risk

Considerable work is being done by many people in defining operational risk and the ways of managing it. Operational risk does not easily lend itself to financial quantification. The nature of operational risk makes quantitative assessment very difficult. However, institutions have initiated steps for measuring operational risk. These include charging a fixed or proportional rate on the cost incurred, using various statistical models based on historic information about losses and loss events.

Box 1: G-30 and Basel Committee Reports on Risk Management

In the past few years, there have been many reports on the issue of risk management and control. Two reports which merit mention are:

1. Derivatives: Practices and Principles, G-30 report published in July 1993.
2. Risk Management Guidelines for Derivatives, written jointly by the Basle Committee on Banking Supervision and the IOSCO.

As per these reports, the fundamental roles for effective management of operational risk are:

- The importance of defining the scope and policy of the firm's involvement in and use of the various financial instruments at the highest level of the organization.
- The need for a risk management process that involves continuous measuring, monitoring and controlling of all risk.
- The need for accurate and reliable management information with comprehensive limits.
- The need for sound control and operational system.
- The need for thorough audit and control procedure.

Source: ICFAI Research Center.

Risk Management Framework

In looking at corporate level risk framework, the organization needs to ensure that the various key areas are in place. These areas include organizational issues and people issues as strategy, structure, people skills and technological issues such as data mining and risk management tools. The organizational issues include development of a risk management strategy, and risk culture, defining management role and responsibilities. When it comes to people issues, the relevant type and caliber of people, the adequate levels of training and development of staff, the basic skill levels come to the fore. And finally, the technology issues include adequate systems to support the various product lines, infrastructure, data warehouse, credit monitoring and credit risk management.

Box 2: Operational Risk – A Hard Nut to Crack

Operational risk arises from the risk of unexpected losses arising from deficiencies in a firm's management information, support and control systems and procedures.

Thus, risk management should focus on the identification of these potential unanticipated events and on their possible impact on the financial performance of the firm and at the limit on its survival.

It is too tempting to classify all those risks that are not included in either the credit risk or market risk as Operational Risk. The Basel Committee's definition or Operational Risk is "the risk or direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition includes legal risk as well. The use of more highly automated technology, the growth of e-commerce, large-scale mergers and acquisitions that test the viability of newly integrated systems, the emergence of banks as very large-volume service providers, the increased prevalence of outsourcing and the greater use of financing techniques that reduce credit and market risk, but that create increased operational risk, all suggest that operational risk exposures may be substantial and growing.

The Basel Committee Report on Operational Risk Management mentions that a few international banks do have systems to measure operational risk but they are yet to the classified as satisfactory or acceptable. Experimental measures adopted by a few banks identified factors like internal audit ratings, volume, turnover, error rates and income volatility as indicators or the levels of operational risk. The management of operational risk is more complicated and requires integration with the other risk management strategies. Internal controls and internal audit are the two basic tools for controlling operational risk.

The Role of Senior Management

The Boards of Directors should approve procedures and controls to implement the polices at all management levels. The senior management should be able to identify and understand the types of risk hidden in the organization activities and to ensure the various lines of business are managed effectively. A good and sound risk management culture within the organization is a must. The managers must have independent access and direct lines of communication with board members. They should be provided with proper training and education to ensure they understand the benefits and risks of various financial instruments like derivatives etc. There should be good and effective rewards for the trading staff or corporate treasurers. In addition to this, there must be a supervisory role to ensure controls and compliance with procedures. Senior managers need to identify adequates segregation of duties between risk management and control personnel.

Risk Management Culture

The concept of risk management within the financial industry has frequently been associated with financial loss or fraud. Generally these occur when something wrong takes place or when an organization incurs substantial loss. This will lead to preoccupation and excessive focus on administrative processes and controls rather than outcomes and performances. This creates fear, uncertainty and suspicion among the staff. In order to make risk the responsibility of the staff at all levels the organization needs to develop a risk management culture. This means that system and process are designed with risk management in mind while staff development and training focuses on effective risk management practices, as this alone will ensure that the organization will be able to manage risk effectively.

Enterprise-wide Co-ordination

In order to effectively manage enterprise-wide-risk, the risk management functions need to have cross-functional responsibility with a direct reporting line to the Board of Directors. This allows the co-ordination of risk management across different business units. Effective coordination in the organization helps establish and communicate risk policies in a better and effective way.

Box 3: Models of Operational Risk

Operational risk measurement techniques fall under two basic approaches namely top-down approach and bottom-up approach. The first approach takes aggregate targets, such as net asset value or net income to analyze the operational risk factors and loss events that cause fluctuations in the target. The second approach disaggregates the targets into many sub-targets and evaluates the impact that factors and events have on these sub-targets.

TOP-DOWN RISK MODELS

Top-down models focus on aggregate measures of an organization's performance.

It involves the following steps:

1. Identifying target variable.
2. Identifying major external factors and events that influence the target variable.
3. Developing a model of the dependencies between the target and the risk factors and events.
4. Calculating operational risk as the variance in the target that is unexplained by the external factors or as the variance that is explained by some operational factor.

Simplicity and low resource requirements are major benefits of top-down approaches. Limitations are, in general, less relevant for operations managers because the source of the operational loss is not made explicit and is therefore not actionable. These models that estimate operational risk as a residual are always backward looking; it is difficult to extrapolate the results to the next period.

Stock Factor Models

Analysts can use the current market value of equity as a performance target if the business is publicly traded. This approach requires estimating the sensitivity of the stock's rate of return to different factor returns for estimating a stock's beta.

Stock-based approaches can be modeled quickly and inexpensively like all top-down approaches. This process is transparent and requires few assumptions about accounting conventions.

Income-based Models

Income-based models measure operational risk in an effective and inexpensive way, if the management's focus is relatively short-term and immediate and if the income statement protection is paramount, and also when historical earnings are available.

Similar to the stock based models, operational risk is assessed as a quantitative residual after the external factors like historical market, industry, and credit factors have been removed from the historical earning fluctuations.

These models are quick to construct and easily comparable assuming that historical data is available. These models incorporate diversification across business areas and as a result are easily used for capital allocation.

Expense-Based Models

These models are the simplest approach for identifying Operational risk, its measurement, and analysis. These models associate operational risk with variations in historical expenses. Operating cost instability refers to the operational errors, fines, and losses that a business may incur during its operations. These are normally posted to the P&L accounts in the general ledger. The main benefits of these models are their ease and low cost. Focusing on operating costs the model overlooks the non-expense risks such as reputational risks, opportunity costs, or those losses that decrease revenues.

Operating Leverage Models

Operating leverage risk is the risk of a less-than-perfect match between revenue fluctuations and expense fluctuations. It depends on the size of the asset base relative to operating expense. Proxies for operating leverage are simple functions of the fixed assets and the operating expenses. Though an important component of operational risk, Operating leverage risk does not include many other aspects of operational risk like risk due to failure of internal controls etc.

Scenario Analysis

Scenario analysis gives us a qualitative technique for understanding the impact associated with major operational and business events and for developing emergency plans to respond. It builds a number of scenarios describing a particular combination of events that could occur in the future. Some of these scenarios describe that huge credit and market losses are external shocks, while some others describe Critical systems failure, major regulatory changes, loss of key people, or class legal actions as some of the internal shocks. The goal of Scenario Analysis is not prediction but prescription. It is useful when there is extreme uncertainty and lack of clarity.

Risk Profiling Models

Risk profiling models focus on tracking a handful of risk indicators that reflect process or system health. No attempt is made to link these factors to any target variable. Some of the measurements include: ratio of contractors to staff, supervisory ratio, down time, number of limit violations, number of temporary procedures, average years of staff experience, backlog levels, backlog of change requests etc.

If consistent measures are used, profiling models would be good for analyzing the evolution of operational risks over time, thus allowing the operations managers to deal with the problems before they get out of hand. The downside of profiling is the absence of a link between a target variable and the risk indicators that makes factors arbitrary. It also shifts focus onto the symptoms rather than the causes of the problems.

BOTTOM-UP RISK MODELS

These models begin with the basic elements of operations, such as assets and liabilities or processes and resources, and in a bottom-up fashion describe how potential changes to these elements could affect targets such as mark-to-market asset values and net income.

Several steps involved in designing a quantitative bottom-up model are:

- Identifying a target variable
- Identifying a critical set of processes and resources
- Mapping those processes and resources to a combination of risk factors and loss events for which historical data is gathered
- Stimulating the potential changes in risk factors and events over the time horizon
- Inferring from the mapped and the stimulated changes, the effect on the relevant target variables.

Bottom-up models are general in that they can be integrated with other models used for operational management. Asset-based models are often more accurate than other models but require more time and resources to develop. They require detailed data about specific losses that can affect the assets and liabilities in the organization. These rely heavily on the Pareto Principle. It follows that analysis should focus on the most critical assets and liabilities.

SELECTING A RISK MODEL

Various risk modeling techniques should be seen as complementary rather than as substitutes for one another. As systems and data have become more widely available, and managers have become more familiar with different techniques, some trends have become evident. A survey in 1999 suggests a dim progression from the trust on skilled audit staff towards more proactive, quantitative, bottom-up models.

It helps to consider some common examples to understand better the bottom-up approach:

- **Asset Liability Management:** Traditional asset-liability management looks at projected future earnings in a number of financial scenarios. ALM approaches are most appropriate for those assets that are not marked to market.
- **Market Factor Models:** Knowing the distributions of factor returns for a short time horizon, the mapping between assets and risk factors, the initial value of the asset allows us to estimate the distribution of asset values in the forthcoming time period.
- **Actuarial Loss Models:** These models are used to estimate the random incidence of claims when an insured party suffers damages that are partially covered by an insurance contract.
- **Casual Models:** These models combine data about historical losses with subjective casual relations to produce estimates of conditional probabilities of one loss event, given that another has already occurred.
- **Stress Tests:** These are quantitative and shock the system to discover the impacts of the stresses. The key risk factors are stressed or given values beyond their normal operating ranges to reveal differences in processes and systems that might lead to unexpected errors.

Strengths

Top-down Models:

- Focus on cost management; are simple; and inexpensive to implement.
- Focus on long-term strategy involving great uncertainty or ambiguity.
- Use publicly available data.
- Are theoretically, simple to perform.

Bottom-up Models:

- Focus on balance-sheet protection, and are relatively accurate.
- Are long-term focused.
- Focus on market risk management.
- Are highly relevant to operations managers.

A hybrid approach combines the best of multiple methods. For instance, it incorporates:

- Factor models, which are used in income-based models.
- Loss events, which are used in asset-based models.
- Actuarial techniques, which are used in insurance actuarial models.
- Casually related events, which are used in casual models.

Source: Measuring and Managing Operational Risk in Financial Institutions, by Cristopha Marshall.

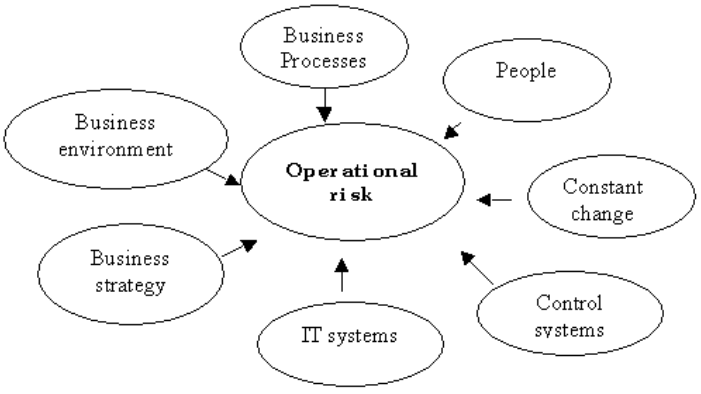
MAJOR SOURCES OF OPERATIONAL RISK

Risk is inherent in every business and is equally applicable to a small local area bank as it is to a giant public sector bank. In order to pursue business opportunities to earn returns for their owners, banks undertake risks. Therefore, operational risk emanates from the business processes, from people who carryout these processes, from the internal control systems that govern these operations, from the strategy adopted to carry out the business, from the environment in which the said business is carried out, etc. However, a deeper look at each of these elements is essential to build a resilient organization that can manage operational risk on a dynamic basis.

Business Process

The loss under this head arises more out of failure of business delivery process, breakdown or other disruptions in technology. The pre and post-stages of transaction process of every business activity undertaken by a bank are potential enough to cause losses. These processes can result in an error or fraud inflicting losses on the organization. Incorrect execution of a transaction could be due to the product-complexity or the incapacity of the people to execute the transaction or the failure of the Management Information System to capture the wrong processing of the transaction well in time. Losses could also arise by virtue of people executing the transaction outside their delegated authority or beyond the boundaries of laid down policies and procedures. They may also arise solely on account of fraudulent intentions of the other party of the transaction that has incidentally gone unnoticed. At times, staff may also connive with outsiders in defrauding banks.

Figure 1: Operational Risk: Sources of Risk



Source: GRK Murty, Operational Risk Management in Indian Banks: A Critique – IJBM – February, 2003.

People

People manning the banking transactions are potential enough to cause operational risk for they can intentionally or unintentionally cause losses by way of "employee-error" or misdeed etc. This potential is further accentuated by the way in which a bank manages its employees. Poorly trained or overworked employees may inadvertently expose a bank to operational risk.

An individual's disposition – inborn personality traits – help define whether someone is a risk taker or not. Generally, greed and fear are identified as the key drivers of behavior. Greed leads to a focus on big wins. Fear concentrates the mind on averting loss. And both the traits are potential enough to create problems to banks and in turn threaten their profitability.

Staff members' experiences relating to big gains and losses – particularly when they occur early in the career, shape their future orientation towards risk-taking. It shapes an employee's views on himself and his abilities, leading to misperceptions and superstitious thinking about oneself. This trait is glaringly visible in the traders' community of banks, who by these experiences may well consider themselves as skilled or lucky while those who lose money become more vigilant in looking for problems with the market or their colleagues. All this gets further flared-up owing to the kind of competitive stress that the bank staff are subjected to.

Management reward systems are also known to encourage bank staff, particularly the traders segment, to meet targets by taking a controlled amount of risk, cutting loss-making positions and repeating winning strategies. Sometimes behavior deviates from this pattern. Traders may, for example, set their own agenda and seek or avoid risks accordingly. When such self-drawn agenda is not in congruence with the organizational interests, employees are likely to create new risks to the bank.

Recent studies have reiterated that operational risks are embedded in human nature i.e., the kind of skills that employees bring to their workplaces. Research indicates that risk taking in any domain is influenced by a combination of general factors such as age, sex, desire to seek sensation, values, openness, etc of the people who are entrusted with the responsibility of managing the business. Risk behavior is mostly patterned – some are likely to be constant risk takers, while others are consistently risk averse, while a third group may have a domain specific pattern of risk behavior.

Most people take risk in order to reap some psychological or material benefit, not for the sake of the risk itself. People with high consciousness will perceive these benefits through disciplined striving rather than taking risks. People with low consciousness are often noticed attempting to secure quick results by taking chances rather than controlled effort, and in the process expose the bank to risk. Some people in their obsession for career progression, ambitiously pursue business targets with a myopic focus and in the process expose the organization unwittingly to greater risks.

The ethical profile of staff that describes one's diligence in exercising powers, tendency to transgress authority/violate norms, commitment to the institution's interest, ability to own up the responsibility, etc., also plays a great role in causing or averting operational risk. There are umpteen instances where people have flouted the delegation. The potential of an employee for such offences is defined by the individual risk propensity, competency and personality profile. A personal profile that is endowed with traits such as – extramarital affairs; drug, alcohol, or gambling addiction or debts; extraordinary medical expenses; regular travel and entertainment expenses of high proportions is known to predispose an individual to commit unethical practices, including committing frauds, besides clouding the individual's very thought process.

It is interesting to recall what Emile Durkheim[1] once reasoned out: "Where a person's aspirations are balanced by opportunities, a state of contentment exists. On the contrary, he suggests that crime breeds in the gaps between opportunities and aspirations. Where aspirations cannot be fulfilled through legitimate opportunities, unconventional methods will be sought". This assertion concludes that people who are prone to committing frauds are endowed with characteristics such as being usually resentful of their employer organization, unfulfilled financial expectations, contributions are not properly recognized; have a basic disrespect not only for their superiors but also for their colleagues; have little or no respect for their employer's property; etc.

Ironically people prone to commit frauds are often perceived by the management as hard working while the perpetrators of fraud often believe their managers to be stupid, weak and amoral. Motivation, being influenced by external social forces, changes from time to time. That is one reason why a known honest man of today, turns a criminal the next day and having over stepped the line once, is likely to repeat the behavior. Although, the rapid changes in the structure of the society and in the structure of crime are known to run on parallel lines, it is very difficult to quantify the effect of social pressures on individual's motivation.

Secondly, the opportunity for an individual to defraud an organization depends on one's access to assets, systems and/or records of the organization; skills – higher the level of skills, higher the risk; right time – a fraudster selects the time and the place looking for weaknesses in the fraud-defense-mechanisms; and his rank in the organization that facilitates bypassing of controls and intimidation of subordinates so that, the irregular conduct of the employee is not reported to the top brass.

The skills that are very critical in defining an individual's style of discharging the assigned role from out of which operational risks are likely to emanate can be traced to three broad categories:

- Risk profile of a person –

  Risk loving/averse,

  Healthy, able to bear stress/easily burnt out,

  Highly ambitious of achieving business targets,

  Obsessive about career progress.

- Skill profile of a person –

  Technical competency to carry out the assigned role,

  Zeal for learning,

  Grasp over the business-environment and client profile,

  Managerial skills such as decision-making, sharing of knowledge, and training the subordinates.

- Ethical profile of a person –

  Commitment to the institution's interest,

  Diligence in exercising powers,

  Ability to own the responsibility,

  Tends to transgress authority/violate norms.

Any incongruence between an individual's risk-profile and the demands of a given role in the bank is potential-enough to cause operational risk.

1 "Forensic Accounting – How to investigate Financial Fraud", William T Thornhill, Synergy books international, Malaysia.

Internal Control Systems

Control is a process effected by the management to provide reasonable assurance to achieve the stated objectives with due diligence regarding reliability on financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations. The major components of internal control are: Control environment, risk assessment, control activities, communication about and monitoring of risk management, as operational risk can arise from any of these segments.

People who are supposed to carry on the business within the framework of prescribed control systems must be made fully aware of the risk involved in the business they are carrying out and its vulnerability to financial crimes, so that they can devote their attention to prevent it by undertaking appropriate measures. Financial crimes such as a fraud or rogue-trading being opportunistic in nature often arise when the systems and controls are operationally inadequate to arrest them. For example, a bank is susceptible to money laundering when its staff does not know the customer or has failed to implement the prescribed procedure in identifying the customer.

Control Environment

The basic elements of control environment that set the tone of a bank in influencing the control consciousness of its staff are:

- Integrity and ethical values,
- Commitment to competence,
- Human resource policies and practices,
- Assignment of authority and responsibility,
- Management philosophy and operating style,
- Participation of the audit committee and
- Organizational structure.

Any weak spot under these items is quite capable of impacting operational risk to the detriment of the bank.

Risk Assessment

It is often addressed by the internal audit system of a bank. Any failure on the part of the auditors can result in operational risk. Following are some such areas that call for constant vigilance –

- Changes in the operating environment,
- New personnel as unit heads,
- New information system,
- Rapid growth,
- New technology,
- Corporate restructuring,
- Regulating pronouncements.

Control Activities

At times the very rules and regulations introduced to arrest operational risk may ultimately result in the same. Some such areas are –

- Performance reviews – reviewing the actual performance against the budget.
- Information processing – controls that check accuracy, completeness and authorization of transactions.

- Physical controls – activities that assure physical safety of assets and records.
- Segregation of duties – authorization, record keeping and custody.
- Any top management slack in effectively using the information available through these control mechanisms, allows operational risk to go unnoticed and be managed in time.

Information and Communication: This involves methods and records established to record, process, summarize and report branch level transactions to top management. It also includes maintenance of accountability relating to assets and liabilities. Any let-up in executing acts such as the following can result in risk:

- Identifying and recording all valid transactions.
- Proper measurement of values,
- Recording in the proper time period,
- Presenting properly,
- Communicating responsibilities to employees.

Monitoring

It is meant for assessing the quality of internal control performance over time. It is an ongoing process that involves reporting by branches to top management from time to time or separate evaluation or a combination thereof by internal/external auditors. Traditionally, auditors assess the efficiency of management control and trigger enforcement activities to correct any deviations.

"Auditing" is the major internal control system that is used in banks to check compliance with the laid down procedures/policies and detect errors, if any, in the business processes carried out across the system that too well in-time before they grow into a catastrophe. One of the best practices internationally prevalent in the audit area is to use the best people in audit. In our context, this is perhaps still a far cry. Because even today, a post in the Inspection and Audit department is generally perceived by the staff as an end to their career progress. Such ill feelings would obviously reflect in the output of auditing. All this cumulatively raises the following questions:

- Are audit reports adding value?
- Audit reports are diagnostic test reports but the question is – are they used as such? And the answer is obvious: Year after year audit reports are being closed with certain exemptions hoping that branches will rectify them in due course. However, they again find a place in the subsequent audit report and the exercise continues. To that extent, auditing and closure of audit reports have perhaps become an annual ritual.
- Is it not the job of auditors to unearth frauds and if so, how do frauds continue to occur even in branches where concurrent auditing is in force?
- Auditing of large credit, forex, investment portfolios, etc., calls for specialized knowledge and competencies in the respective field, but the question is, do auditors have such specialized skills? Suffice to say that so long as Inspection and Audit departments are treated as parking slots for inefficient people, internal control and supervision shall continue to suffer and in turn operational risk continues to haunt the banks.

Thus, monitoring is very critical in arresting operational risk at the branch level.

IT Systems

As technology has become all-pervasive in business, IT risks are becoming increasingly entangled with business risks. Technology changes quickly and continually provide new capabilities that banks want to take advantage of in their businesses. But new technology, as a general rule always remains a few steps ahead of the ability of the people to use it and therefore exposes a bank to risk.

Technology, people often say, is the automation of business processes that resolve, operating risk by eliminating the human error. But research reveals a contrarian perspective i.e., IT may not eliminate operational risk totally. "It is reported that the possibility of greater anonymity resulting from electronic or computer communication has reduced saboteurs' fears of being identified and getting caught. The consequence of anonymity is that those interpersonal deterrents that in the past fostered an employee's concern for "looking right" in front of co-workers are now rapidly disintegrating due to the greater number of interpersonal transactions that organizational members conduct electronically inflicting more financial losses".

Another example of operational risk emanating from IT systems is the absence of "visibility" in the system like in settlement; if there is a trade failure, exception management may not be available to enrich and overcome that failure. It may not be wrong to say that IT professionals in banks generally do not have the technical and managerial skills necessary to help banks shift from older technologies to new ones smoothly. They also lack skills to integrate technology with business. Any over-reliance on technology experts is therefore likely to result in faulty investments or disruption in business processes that can result in "lost-opportunities."

Research studies indicate that computer-savvy people have a seemingly inbred dislike and disregard for authority. As they often work around problems, they like to find shortcuts to get a job done or a problem solved. In the process, they turn to be resentful of what they consider to be artificial barriers imposed by middle level managers who have very limited knowledge of the modern computer technology. This poses two threats: one, the tech-savvy juniors "look down" on their managers and even challenge their authority; and two, managers may fail to check the work of their subordinates in the area of computers, for that matter in any specialist areas.

Of late, Indian banks have started offering e-banking which is a Web-based service that enables the bank's authorized customers to log on to the banks website with the help of the bank issued identification and a Personal Identification Number (PIN). Internet, a public network of computers that facilitates free flow of the data/information with unrestricted access, if it is being used by banks as a medium for offering e-banking services, can introduce security risk into the business. It is important to understand that no bank is immune to security breaches that can damage its credibility, customer confidence, and ultimately its reputation.

The security concerns of e-banking emanate both from internal and external sources: Insecure passwords, disgruntled employees, viruses, inappropriate use of e-mail constitute internal security problems while, external risks are introduced by the Web or e-mail. Unauthorized access to a bank's critical information stores like accounting system, portfolio management system etc., could result in direct financial loss to the bank. For example, hackers could access, retrieve, and use confidential customer information or introduce virus. This can cause loss of data, tampering with customer information, etc., that are potential enough to damage the reputation of the bank besides creating legal implications by virtue of infringing customer's privacy. In the Internet environment, attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill-seekers.

Business Strategy

According to Chandler, "Strategy can be defined as the determination of the basic long-term goals and objectives of an enterprise, and the adoption of courses of action and the allocation of resources necessary for carrying out these goals…" Learned et al., defined strategy as "the pattern of objectives, purposes, or goals, and major policies and plans for achieving these goals, stated in such a way as to define what business the company is in or is to be in and what kind of company it is or is to be?.."

During the early 1990s, when capital market was said to be in boom, many banks floated mutual funds making tall promises like doubling or tripling of investments to their investors. No one bothered how these promises could be fulfilled if capital markets crash which had literally happened subsequently. Canara bank, Indian bank and State Bank of India are some of the banks that have suffered heavily by virtue of adopting a short-sighted strategy of not having a properly evaluated strategy beforehand.

Similarly, launching of a new product without a properly articulated strategy is likely to end-up in disaster. Any major change in business strategy usually requires a change in organizational structure as well as changes in the information and control systems, attitudes, training requirements of staff, etc. Unless these issues are properly addressed, there is every likelihood of banks suffering from operational risk. At times, the change management initiated by the CEO may itself inflict financial losses by virtue of alienating the operating staff from the proposed change for reasons galore. The strategies designed and put in operation may at times fail to deliver the intended returns resulting in lost opportunities. Such weak strategies may be due to lack of competency or poor leadership at the top.

Business Environment

The environment in which banking is carried out will have its own say on the operational risk. For example, it is reported that one of the reasons for poor loan recovery rate in the eastern parts of India is the prevailing poor law and order situation. Similarly, physical security to the assets of the banks is considered quite poor in states where the law and order situation is far from desirable. Natural disasters like recurring cyclones, floods, etc., also inflict losses on the system. Terrorist threats, strikes and the predisposition of people for civil-litigation also matter in operational risk.

Outsourcing

Today, banks are resorting to outsourcing some of their activities, particularly in the IT segment and this may in certain circumstances help reduce the operational risk faced by a bank. However, banks may lose control over the quality of performance of outsourced activities unless the contract is well drafted. Secondly, as a sequel to outsourcing, a bank may lose its ability to conduct them in-house, particularly if the staff with that vital expertise is lost. This may pose a serious threat to the continuity of its operations if the service providers fail to perform.

Rate of Change in the Business Environment

During the last ten years banks have found it necessary to embrace a program of almost constant change, encompassing downsizing, business process reengineering, new technology, mergers and acquisitions, outsourcing and so on. Experience has shown that an organizational exposure to operational risk tends to increase as the rate of change increases and individual change introduced interact with each other creating an impact at the level of the organization.

The rate of change can alter the risk profile of a bank and by doing so, catch the management and staff by surprise. Similarly, the increased mergers and acquisitions activity is also perceived to have increased the bank's overall exposure to operational risk. This increase is mostly felt during the post-merger period. In the case of merged units, operational risk has been traced to (Chris Frost, David Allen, James Porter and Philip Bloodworth, 2001):

- Reduced levels of appraisal management supervision including transaction volumes, with risk swamping the operational processes; and
- Changes to overall business relationships with increasing cross-organizational dependencies and the attempt to integrate working practices, systems and cultures that were not designed to work together.

MEASUREMENT OF OPERATIONAL RISK

To begin with, a bank has to understand its operational risk profile by first identifying the types of operational risk that it is exposed to. Operational risk usually spreads across the following:

- Nature of bank's customers, its products and activities, distribution/service delivery mechanisms, complexity and volumes of transactions.
- The design, implementation and operation of the processes used in the end-to-end operating cycle for a bank's products and activities.
- Risk culture and human resource management practices.
- Business operating environment – political, legal, socio-demographic, technological and economic factors; competition and market structure.

As operational risk emanates from internal operational performance factors, it has remained fuzzy, making risk quantification difficult. Hence, it is difficult to build a clear mathematical or statistical link between individual risk factors and the likelihood of a loss. At the same time, inadequate management of operational risk has potential adverse implications for all banks as it can affect their solvency, adequacy to discharge their obligations to the customers and their susceptibility to financial crime. As on date, it is an acknowledged fact that due to both data limitations and a lack of analysis tools, a number of operational risks cannot be measured accurately in quantitative terms. Hence, banks are resorting to the process of risk assessment in terms of "high, medium and low" rather than risk measurement.

The accumulated experience indicates that there are two broad categories of operational losses –

- Frequent, small operational losses that may result from human error, which are quite common to all businesses.
- Major operational risk losses resulting from actions beyond the delegated authority or outside the laid down procedures, as reported in the Madhavpura Case. They are of low probability but their impact could be very large.

The Basel Committee in the revised consultation paper on its proposal for operational risk capital requirements, to be introduced as part of the Revised Accord, suggested three possible approaches to the calculation of operational risk capital.

Basic Approach

It uses a fixed percentage ("alpha") of gross revenue in a range of 17 – 20%.

Box 4: Basic Indicator Approach
The most basic approach allocates operational risk capital using a single indicator as a proxy for an institution's overall operational risk exposure. Gross income is proposed as the indicator, with each bank holding capital for operational risk equal to the amount of a fixed percentage, "α", multiplied by its individual amount of gross income. The Basic Indicator Approach is easy to implement and universally applicable across banks to arrive at a charge for operational risk. Its simplicity, however, comes at the price of only limited responsiveness to firm-specific needs and characteristics. While the Basic Indicator Approach might be suitable for smaller banks with a simple range of business activities, the Committee expects internationally active banks and banks with significant operational risk to use a more sophisticated approach within the overall framework. The current provisional estimate is that "α", be set at around 30% of gross income. This figure needs to be treated with caution as it is calibrated on a limited amount of data. Also, it is based on the same proportion of capital (20%) for operational risk as the Standardised Approach and may need to be reviewed in the light of wider calibration. For instance, in order to provide an incentive to move towards more sophisticated approaches, it may be desirable to set "α" at a higher level, although alternative means of generating such an incentive are also available. For instance under Pillar 2 or by making the Standardised Approach the entry point for internationally active banks. It is also worth noting that a sample of internationally active banks has formed the basis of this calibration. As it is anticipated that the Basic Indicator Approach will mainly be used by smaller, domestic banks, a wider sample base may be more appropriate.

Source: Basel Committee on Banking Supervision, Consultative Document Operational Risk, Supporting Document to the New Basel Capital Accord Issued for comment by 31 May 2001, January 2001.

Standardized Approach

It is same as the Basic Approach, but fixes different percentages for different types of businesses such as retail banking, asset management, etc.

Box 5: Standardised Approach
The Standardised Approach represents a further refinement along the evolutionary spectrum of approaches for operational risk capital. This approach differs from the Basic Indicator Approach in that a bank's activities are divided into a number of standardised business units and business lines. Thus, the Standardised Approach is better able to reflect the differing risk profiles across banks as reflected by their broad business activities. However, like the Basic Indicator Approach, the capital charge would continue to be standardised by the supervisor. The proposed business units and business lines of the Standardised Approach mirror those developed by an industry initiative to collect internal loss data in a consistent manner. Working with the industry, regulators will specify in greater detail which business lines and activities correspond to the categories of this framework, enabling each bank to map its structure into the regulatory framework. It is needed to ensure that businesses are slotted into the appropriate broad categories to avoid distortions and the potential for arbitrage. Within each business line, regulators have specified a broad indicator that is intended to reflect the size or volume of a bank's activity in this area. The indicator is intended to serve as a rough proxy for the amount of operational risk within each of these business lines.

Source: Basel Committee on Banking Supervision, Consultative Document Operational Risk, Supporting Document to the New Basel Capital Accord Issued for comment by 31 May 2001, January 2001.

Advanced Measurement Approach

Under this Approach, banks will be permitted to use their own internal model to calculate required capital. Banks are obviously, in a dilemma as to how to implement the "advanced model approach". The consultation paper has however identified three forms of models for estimating operational risk viz. Internal Modeling Approach, Loss Distribution Approach, Score Card Approach.

Box 6: Advanced Measurement Approaches

The AMA is the most risk sensitive of the approaches currently being developed for regulatory capital purposes. The Committee has developed the concept of Advanced Measurement Approaches in recognition that a variety of potentially credible approaches to quantifying operational risk are currently being developed by banking institutions and that the regulatory regime should not stifle innovation at this critical point in the development process. The regulatory capital requirement for operational risk under the AMA would be based on an estimate of operational risk derived from a bank's internal risk measurement system. This risk estimate would be subject to a floor based on the Standardised Approach capital charge for operational risk.

Thus, under the AMA, banks would be allowed to use the output of their internal operational risk measurement systems, subject to qualitative and quantitative standards set by the Committee. In many regards, this structure – the use of internally generated risk estimates subject to qualitative and quantitative standards – mirror the structure of the internal models Under the AMA, operational risk capital charges would be subject to a floor based on the Standardised Approach capital charges for operational risk. Initially, this floor would be fairly stringent, reflecting the fact that the internal methods used to quantify operational risk are still in early stages of implementation and that the AMA do not, as yet, contain detailed criteria for the specific quantification methods likely to be used by banks. It is proposed that the floor be set at 75% of the Standardised Approach capital charge. However, the intention would be for the Committee to revisit developments in this area on a regular basis – perhaps every two years commencing from the release of the final revisions to the Accord. With the intention of identifying those measurement approaches that have been developed most rigorously by the banking industry more detailed qualitative and quantitative standards could be developed based on the emergence of sound industry practices in areas such as measurement and validation techniques. The floor could be lowered, and eventually eliminated, for approaches meeting these more detailed standards.

A key purpose of incorporating the AMA concept as one of the methods under Pillar 1 is to allow the development of a range of nascent capital assessment techniques. The Committee would however be interested to gauge which of the current range of techniques is most likely to be developed by a critical mass of banks in the foreseeable future, and allow focus to be given to its work over the coming months and years. In order to assist in this process, the committee is setting out its current understanding of the range of possible approaches under an AMA type framework.

Source: Basel Committee on Banking Supervision Working Paper on the Regulatory Treatment of Operational Risk, September 2001.

Internal Modeling Approach

Under this method the expected losses in each business line are calculated by examining the average of past losses experienced, and then multiplied by a standard "gama" factor to derive a figure for unexpected or worst case losses which give the capital requirement.

Box 7: Internal Modeling/Measurement Approach
The Internal Measurement Approach provides discretion to individual banks on the use of internal loss data, while the method to calculate the required capital is uniformly set by supervisors. In implementing this approach, supervisors would impose quantitative and qualitative standards to ensure the integrity of the measurement approach, data quality, and the adequacy of the internal control environment. The Committee believes that, as the Internal Measurement Approach will give banks incentives to collect internal loss data step by step, this approach is positioned as a critical step along the evolutionary path that leads banks to the most sophisticated approaches. However, the Committee also recognises that the industry is still in a stage of developing data necessary to implement this approach. Currently, there is not sufficient data at the industry level or in a sufficient range of individual institutions to calibrate the capital charge under this approach. The Committee is laying out, in some detail, the elements of this part of the approach and the key issues that need to be resolved. In particular, in order for this approach to be acceptable, the Committee will have to be satisfied that a critical mass of institutions have been able, individually and at an industry level, to assemble adequate data over a number of years to make the approach workable.

Source: Basel Committee on Banking Supervision, Consultative Document Operational Risk, Supporting Document to the New Basel Capital Accord Issued for comment by 31 May 2001, January 2001.

Loss Distribution Approach

As in the case of VaR, this method attempts to fit a statistical distribution of the historical losses and derives the capital requirement from a confidence level on this distribution.

Box 8: Loss Distribution Approach (LDA)
Under the Loss Distribution Approach, the bank estimates, for each business line/risk type cell, the probability distribution functions of the single event impact and the event frequency for the next (one) year using its internal data, and computes the probability distribution function of the cumulative operational loss. The capital charge is based on the simple sum of the operational risk VaR for each business line/risk type cell. Correlation effects across the cells are not considered in this approach. The loss distribution approach has the potential advantages of increased risk sensitivity. This method differs from the Internal Measurement Approach in two important respects. It aims to assess unexpected losses directly and not via an assumption about the relationship between expected loss and unexpected loss, and the structure of business lines and risk types is determined by the bank itself. There is no need for the supervisor to determine a multiplication (gamma) factor under this approach. At present, several kinds of measurement methods are being developed and no industry standard has yet emerged. In this circumstance, basing the capital charge on the bank's own methodology will cause comparability problems because the outcome may differ depending on the method used. Further, it is not clear that many banks yet have the data or methodology to perform the necessary estimations. However, by accepting only those measurement methods that attain a certain level of robustness, over time, it may be possible to establish a set of standards on the basis of which supervisors can secure the overall prudence of the capital framework.

Source: Basel Committee on Banking Supervision, Consultative Document Operational Risk, Supporting Document to the New Basel Capital Accord Issued for comment by 31 May 2001, January 2001.

Scorecard Approach

Under this method banks start estimating historical loss data as in the previous two methods, but also takes into consideration the future risks such as staff turnover and the qualitative assessments of the banks' control environment.

Box 9: Scorecard Approaches
In this approach, banks determine an initial level of operational risk capital at the firm or business line level, and then modify these amounts over time on the basis of scorecards. These scorecards are intended to bring a forward-looking component to the capital calculations, that is, to reflect improvements in the risk control environment that will reduce both the frequency and severity of future operational risk losses. The scorecards may be based on actual measures of risk, but more usually identify a number of indicators as proxies for particular risk types within business units/lines. The scorecard will normally be completed by line personnel at regular intervals, often annually, and subject to review by a central risk function. In order to qualify for the AMA, a scorecard approach must have a sound quantitative basis, with the overall size of the capital charge being based on a rigorous analysis of internal and external loss data. In some cases, scorecard approaches are based on initial estimation methods that are similar to those used in internal measurement or loss distribution approaches. Where the scorecard approach differs from these approaches is that it relies less exclusively on historical loss data in determining capital amounts. Instead, once the size of the capital charge has been determined, its overall size and its allocation across business lines may be modified on a qualitative basis. Nevertheless, historical loss data must be used to validate the results of scorecards, with adjustments to capital size or allocation based upon such results. At present, a range of scorecard approaches are in development with some banks already operating a system of economic capital allocation based on such an approach. However, as with the other approaches, no industry standard has emerged.

Source: Basel Committee on banking supervision. Working Paper on the regulatory treatment of operational risk, 2001.

Amongst the three models, globally, the scorecard approach is perceived as an attractive approach, for, it offers the following advantages:

- It provides a more complete and accurate measure of operational risks, by incorporating forward-looking risk indicators and qualitative assessments of the control environment as well as loss data.
- It gives managers much stronger incentives to reduce risks, and much better tools to help them identify how to do so.
- It is much easier to implement and also easier to adapt as the requirements of the bank and the regulators, evolve over time.

The Internal Modeling and Loss Distribution approaches have two major defects (James Ward, PA Consulting Group, 2001): they fail to take account of loss types that have not yet occurred and secondly, they fail to adapt to recent changes in the risk environment that have altered the probability or likely impact of events. As against this, the scorecard approach captures these two issues by focusing on general risk classes and on the risk factors that are internal and external to the bank, that drive the probability of these risks. There is however an element of "subjectivity" under the scorecard approach in assigning weightage to each item.

That being the fuzziness of operational risk measurement, it is too early to build up a formal statistical relationship between operational risk drivers and losses and hence, one has to intuitively make a good decision for the time-being and with enriching experiences build up better statistical models later.

MANAGEMENT OF OPERATIONAL RISK

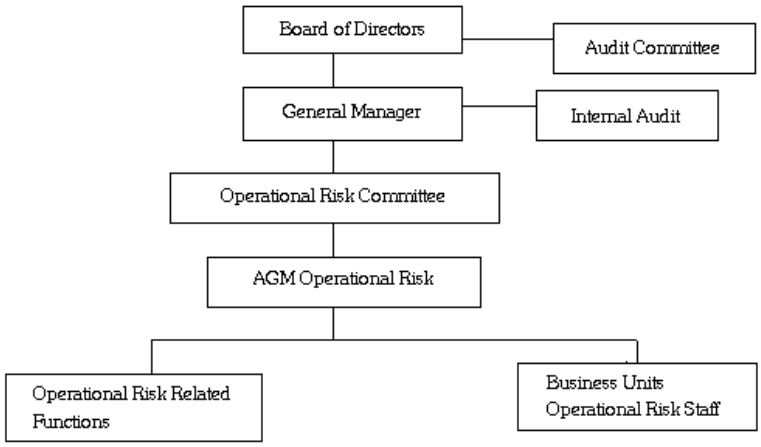
Customer satisfaction in banks has assumed the status of key "differentiator", separating them from the competitors. Operational Risk management can play a vital role in ensuring that managers systematically improve customer service by exercising strict rein over operations and service delivery.

The senior management has to take over the responsibility of creating awareness about operational risk management and ensure that it permeates the whole organization through effective communication channels. It has to build a resilient organization with clearly defined management models and objectives. The internal audit reports and other regular communication to the top management must be able to provide adequate information on branch-wide efforts in managing risk.

It is universally agreed that besides the active participation of the top management from the corporate office in operational risk management, the primary responsibility of operational risk management must emanate from the business unit i.e., branches. Secondly, highly experienced staff must be inducted into the operational risk management department. The third requirement is to assign the responsibility of overseeing the operational risk management function to a senior General Manager. He shall be made accountable for its organizational wide implementation. The fourth important requirement is to develop specific operational risk management policies, for they alone help establish a framework within which operational risk can be measured, monitored, controlled, and reported. The overall guidance for establishing operational risk management culture and monitoring its enterprise wide management has to be directly under the supervision of board of directors.

A formal structure of Operational Risk Committee on the following lines would be appropriate.

Figure 2: Operational Risk Committee



Source: Operational Risk: the next frontier, 1999.

The operational risk committee shall be entrusted with the responsibility of –

- Determining operational risk policies and definition,
- Assessing cross-enterprise risks,
- Assessing both qualitative and quantitative benefits,
- Establishing linkages of operational risk to credit and market risk,
- Administering self assessment and roll out other tools.

Once established, the committee may design risk management practices on the agreed lines and ensure that they are implemented effectively through a meaningful follow-up.

Process (Operational Delivery) Management

A key aspect of operational risk management is to ensure the smooth continuity of business operations and service delivery; it is nothing but a bank's ability to perform business processes on an ongoing basis. The success or failure to maintain operational continuity without break-up shall therefore be aimed at from a perspective of capacity management, service management, sourcing of funds management, crisis management, human resource management, etc. Effective capacity planning process involves:

- Maintenance of correct level of internal and external resources to meet and support business needs.
- Optimization of resources so that business objectives are met with minimal cost.
- Building up of appropriate level of consistency, reliability and predictability in operations.
- Developing benchmarks for comparing the performance of existing processes with other similar processes, business units or competitors.

Services Management

It is essential for the branches to achieve and maintain "best in class" service delivery levels with processes that are reliable, less costly more efficient than those of the competitors. Recently, many of the top financial firms are moving away from risk-taking to more focused business and fee-based services to generate low-risk income with high return on equity. But, there are certain businesses such as custody, trust, asset management etc., which are low on market or credit risk but high in operational risk. This calls for a sound operational framework to make it quite resilient.

There is however, a direct relationship between capacity management and operational resilience, but over-stretching operations could result in increased operational risks, as the staff may be stressed, demoralized and hence more prone to commit mistakes. If a branch is not built to handle increased output, it would be more prone to operational risks.

Banks have to develop appropriate capacities, planning processes so that the business can meet demands placed on the branch by growth, peak demand periods or unexpected changes in demand. The capacity planning process must result in –

- Availability of correct level of internal and external resources at branches to meet and support business needs,
- Management of operational risks at an acceptable level,
- Optimization of resources so that business objectives are achieved with minimal cost,
- Appropriate level of consistency, reliability, predictability of the operations,
- Flexibility to affect changes in the business without interruptions.

People Management

Inappropriate management of human resources may affect both a bank's and its customer's vulnerability to operational losses. It should therefore establish and maintain appropriate systems and controls to manage operational risks, which is likely to emanate from employees. Focus may be made on the following aspects:

- Bank's operational risk culture and any digression from established culture.
- Contingency plans to carry the work in the event of employee unavailability.
- Ensuring that employees are aware of their responsibilities and role in operational risk management and that they are suitable and capable of performing these responsibilities.

- Segregation of duties, rotation of duties and supervision of employees in the performance of their responsibilities.
- Availability of systems and procedures manuals for the usage of employees.
- Training that enables employees to attain and maintain appropriate competence.
- Review of the fitness and propriety of employees – particularly their honesty, integrity and reputation, competence and capability, and financial soundness, at regular intervals and deploy them based on the review findings.
- Performance related remuneration and scope for its increasing operational risk.
- Compliance with regulatory requirements pertaining to employees' welfare.

Taking a cue from the recent research findings, banks must strive to map the risk-potential of its staff from time to time based on their behavioural-exhibits both within and outside the organizational context, and constantly evaluate their risk-potential as it helps the management in picking right people for right job. Any incongruence between an individual's risk-profile and the demands of a given role in the bank is potential enough to cause operational risk.

Successful operational risk management relating to human resources is more an art than science. As against the philosophy of modern management theory, which believes that majority of people want to work, take pride in their work, prefer to take part in decision-making process and help find creative solutions to problems at the work place, provided an opportunity is given (Heny K S Daryanto and Arief Daryanto), whenever a reference is made to risk control, banks always refer to command and control systems which implies that the employer does not trust the employees. This appears to be obvious, for, the bank staff, influenced by powerful human emotions such as fear and greed, is prone to err as witnessed in the case of Nick Leeson, causing operational losses. Perhaps harder controls at all levels are needed to successfully manage operational risk.

Managing Systems and Controls

Auditing is one of the major tools used by banks to ensure control over operations across the organization. Management must therefore use auditing as a powerful ally and rich source of insight and information to know how the compliance is being effected at all work places and to evaluate the "tone-up" needed, to make it effective dynamically. From an operational risk management perspective, audit reports needed to be necessarily analyzed critically as they provide "early warning signals of potential danger".

But the reality in the Indian banking system being what it is, there is a paramount need for both the management and the managed to change their disposition towards audit to ensure that evolving risks are nipped at the budding stage itself. But the use of internal audit report as a prime source of management of operational risks becomes feasible if only there is a –

- Closer integration of audit with business, which today is abysmally low.
- Greater recognition, importance and impact of internal audit in arresting operational risk.
- Availability of early warning signals to top management for correcting the situations.
- Senior management follow up as a clear message to the operating staff.

This ensures immediate remedy all audit-related problem raised, which in turn improves the effectiveness of systems and controls in arresting operational risk.

It is also necessary to maintain appropriate systems and controls to ensure that no operational risk arises from inadequacies or failures in the delivery process or systems and hence, following issues need to be taken care of.

- Processes and systems used in the end-to-end operational cycle to deliver the services should be properly integrated.
- Processes must enable the bank to comply with regulatory and statutory requirement.
- Stand by arrangements to maintain continuity of operations.
- Put in place indicators that identify system risk and thereby enable the management to rectify and replace them well in time.

New Product Review Process

It is often noticed that banks launch new products without assessing the modification, if any, needed in the delivery process or training needs of staff, etc., for its effective delivery and in the process end-up in losses. It is essential to put in place a system of review so that risk management group evaluates new products/services/processes before they are launched. This is to ensure that necessary prophylactic measures can be designed and communicated to operating units so that the proposed product/modification in the delivery processes, etc., are handled with due diligence.

IT Systems Management

It is true that automation of delivery process to a great extent reduces a bank's susceptibility to certain "people's-risk" such as reduction in human errors, segregation of duties, information security. At the same time it also increases a bank's dependency on the reliability of IT systems chosen. It therefore necessitates establishment and maintenance of appropriate controls to manage IT systems-related risk. To accomplish this task, the management must focus on:

- Organization and reporting structure of technology operations,
- Overseeing by the top management,
- Technology requirements and their inclusion in the business strategy,
- Appropriateness of acquired IT systems,
- Maintenance support for hardware and software,
- Appropriateness of allocation of duties under IT operations,
- Maintenance of an internal documentation of processes and systems.

Information about the systems, their handling, problems faced in handling the technology, innovations that have been applied to overcome such glitches, etc., may exist in many places and forms – physical, electronic or known to employees but not recorded, etc. It needs to be collated at a central place and made available to everyone to be used in managing day-to-day problems. The safe-keep of such knowledge calls for –

Confidentiality: Information is made available only to an authorized person.

Integrity: Safeguarding the accuracy and completeness of information being processed.

Availability: Only an authorized person or system is granted access.

Authentication: The identity of a person processing the information must be verified.

Non-repudiation and Accountability: A system must be put in operation that ensures that the person processing the information cannot deny his action.

The operation of processes and systems may have to be necessarily different to be in alignment with the needs of different geographic locations. Accordingly, a bank's operational risk profile gets altered. Similarly, when a bank has operations in different countries, its risk profile obviously differs from center to center. This needs to be taken cognizance of while drafting the risk management procedure.

Change Management

During the times of significant changes in the organizational set-up, infrastructure and business operating environment, a bank's exposure to operational risk is likely to increase owing to –

- Untrained or demotivated employees or significant loss of employees.
- Undertaking a new business activity or the modification of existing activities.
- Inadequate human resources to carry out routine business activities owing to the prioritization of resources to undertake new business etc.
- Changes in regulatory and legal requirements.
- Process or system instability while catering to the increased demand.
- Inadequate/inappropriate/untested processes following business reengineering.

This needs to be addressed on a different footing: Designing an appropriate reporting structure for managing the change; assessing the adequacy or otherwise of the existing processes and systems to manage the change; and communicating the changes in the systems and controls, if any affected, to all the employees.

Disruptions to the continuity of a bank's operations do occur due to certain exogenous events resulting in loss of resources and failure of processes. In order to avoid such disruptions and maintain continuity of the business, a bank has to undertake measures such as succession planning, systems resilience, dual processing/alternate service providers, contingency arrangements, etc. Essentially, managing operational risks arising out of change in business environment is the prime responsibility of the top management.

Risk Monitoring

As a part of its risk management philosophy, the top management shall call for an appropriate report at regular intervals on the operational exposures, loss experience and authorized deviations from the bank's operational risk policy. They should also ensure to maintain the records of –

- Results of risk identification, measurements and monitoring activities.
- Action taken to control identified risks.
- Assessment of the effectiveness of the risk control tools that are used.
- Actual exposures against stated risk tolerance as defined by the assigned capital.

Operational Risk Policy

A bank should document its policy for managing operational risk. It should spell the strategy and objectives for operational risk management and the processes that it intends to use to achieve these objectives. The document should basically contain –

- Analysis of bank's operational risk profile.
- Risks that it is willing to accept and the risks that it is not prepared to accept.
- How it intends to identify, assess, monitor and control its operational risks.
- An overview of the people, processes and systems being used.
- Assessment of bank's risk exposure for allocating capital.

This not only facilitates a uniform approach towards operational risk management in the bank as a whole, but also functions as a benchmark to measure the performance of individual units under operational risk management.

Introducing Effective Risk Transfer Methods

Banks must be abreast of effective risk transfer methods such as insurance or Alternative Risk Transfer. Traditionally, complex technology risks, financial services' professional liability are all good examples of difficult-to-insure risks. But, in the western world, insurance companies are today offering a variety of products that cover a wide range of operational risks faced by banks. They have

been breaking down the whole gamut of operational risk into five components: Personnel covering adverse impact of improper personnel policies, internal fraud, etc., technology covering the risk of loss resulting from systems unavailability, poor data quality, system errors, or software problems; physical assets covering the risk of damage or loss of physical assets that negatively impact operations; relationships covering the risk of loss resulting from relationship issues such as sales practices, etc.; external covering the risk of loss from external fraud, and offering structured coverage (Roland Avery and Paul Milton., 2000). These facilities are of course not yet available for us. Yet, banks have to put an efficient system in force to at least avail the existing insurance coverage for all the risks that can be transferred to the insurers well in time and monitor for their timely renewals.

Knowledge Management

Banks have a wealth of history. Similarly each branch has its own reservoir of knowledge that can be used as a guide to present and future decision-making. From an operational risk management perspective, the key is to unearth this knowledge and find ways to use it to generate value. In the days of flat and less hierarchical structure, knowledge sharing and communication has gained importance. But it is a difficult resource to identify and manage. Effective linkage between knowledge management and risk management can be built by:

- Conducting training programs that inculcate the habit of open communication, knowledge sharing and problem solving among the branch level staff.
- Developing right environment for people to work together in teams at branches.
- Management should work towards making intangibles into tangibles by paying as much attention to branch level environment.
- Embedding communication and information processes in operational practice to create, transfer and store knowledge.

This enables branches to make use of the earlier experiences to fight out similar risks i.e., they need not reinvent the wheel once again.

SUMMARY

- The chapter discusses the divergence in the definition of operational risk to emphasize how it is still evolving.
- It also discusses identification of various sources of operational risk that could emerge in the pursuit of business opportunities.
- The limitations encountered in measuring operational risk are also highlighted.
- The need for intuitively assessing the potency of varied operational risks in inflecting losses to the banks has also been stressed.
- The essential role of the top management in managing operational risk through a well-designed operational risk management set-up and different avenues that need to be pursued to manage operational risk have been deliberated upon.
- In the ultimate analysis, it is the unit heads, which are to implement the operational risk management practices for achieving the desired results under the policy guidelines issued by the risk management committee.

Chapter XV

Risk Management Strategies

After reading this chapter, you will be conversant with:

- Operational Risk Management Strategies
- Financial Risk Management Strategies
- Systemic Risk Management Strategies
- Risk Limitation
- IT Implementation Challenges

> "We took risks, we knew we took them; things have come out against us, and therefore we have no cause for complaint."– Robert Falcon Scott 1868-1912: 'The Last Message' in Scott's Last Expedition (1913).

Financial institutions and banks engage in different kinds of intermediation functions with respect to denomination, maturity, currency and default-risk. Performing these intermediation functions leads to undertaking various risks like interest rate risk, currency risk, liquidity risk and credit risk. In addition to these, financial institutions also bear market risk arising due to active trading of assets in financial markets.

The area of risk management has assumed special significance in light of the deregulation happening in the financial markets of emerging markets. Even in the comparatively liberalised economies like South-East Asian countries, the deregulation and reforms in financial sector have taken off very recently and there is a need for well thought out and debated ideas to carry out this process smoothly.

Banks and other financial institutions are compelled to adopt a comprehensive risk management practice, thanks to the ever increasing competition and regulatory pressures. Banking industry, in particular, has historically remained as a protected industry in many emerging economies. This is due to regulated deposit, lending rates and restriction on competition. Financial stability occupies center-stage as one of the prime policy concerns for the central banks worldwide at the time when banking operations have been undergoing rapid metamorphosis on global level. There is growing realization about the need for preservation of the safety and soundness of individual financial institutions, especially banks, and of the financial system as a whole. This is important not only for conducting business across national borders, but also for preserving financial stability, given the predominantly bank-based nature of financial systems in emerging markets. Not surprisingly, therefore, banking sector is passing through challenging times.

The industry was very complacent enjoying comfortable spreads. However, the following factors among others compelled banks to change the old ways of doing business:

- Technological advancements.
- Disintermediation pressures arising from a liberalized financial marketplace.
- Increased emphasis on shareholder value.
- Macroeconomic pressures and banking crisis during the 1990s.
- Globalization.

The dividing lines between financial products, types of financial institutions and their geographical location have become less relevant today than in the past. Greater globalization of banking operations in an increasingly market-driven environment has made risk management critical, while lending and deposit-taking have continued to remain the mainstay of banking business. In this rapidly changing business environment, need for identifying the inherent risk an organization faces has become the fundamental principle. The present situation requires more sophisticated and comprehensive controls in order to bring the products more quickly into the market. This is the reason why the paradigm shift is directed from risk control to risk management. The process of risk management provides the company the basis to control their risks coupled with measurement of performance effectiveness. Another dimension is determination of capital allocation of and realization of business advantage, which brings about sustenance and growth of the banking and other financial companies on proactive lines.

In the past, organizations went bankrupt due to reasons that were microscopic such as competition, mismanagement or adverse conditions. It was during the nineties that many of the world's biggest banking companies started suffering losses. The reason was lack of proper risk management systems. But today anybody can individually deal in billions of dollars. So the task before the bank is to reduce the transaction and overall intermediation cost, improve yield of assets and slash both gross and net NPAs. This would be helpful in bringing about a structural transformation in line with the best practices. All these are the areas where sustainability must essentially be viewed in the context of long-term issues.

The challenges that come to the fore among other things are stepping up the income, curbing interest expended and operating expenses, credit risk, diversification in banking activities, portfolio investment, payments and settlement systems, and so on. Such unsettled issues and cognizable dilemmas need to be resolved on the basis of resource-mix, investment opportunities, demanding standards of customers and patterns of shifting value to streamline the banking system as an integral part of the blueprint of development.

Box 1

To get profit without risk
experience without danger
and reward without work
is as impossible as it is to
live without being born.

– A P Goether

For the banking fraternity risk, clearly, is a tiger to ride. All these days' bankers saw risk as something that needs to be controlled or minimized. This approach led to a limited view of viewing risk. In the present banking scene where there is unlimited risk; there is unlimited opportunity, too. The time is ripe for bankers to learn to manage risk for maximizing value.

In the uncertain, volatile and fast changing business environment of the 21st century, banks have to learn to cope with risks of every kind. In a protected market, risk meant one of two or three major things – hedging one self. One was not to worry too much about operational risks, technology risks, political risks, legal risks, contract risks, regulatory risks, strategic risks, and a host of other risks. Basel II has thrown new challenges to the banking industry in managing hitherto un thought of risk areas.

Just setting up a risk management department is not risk management. It's about entrenching a risk culture across the bank. If risk creates opportunities, opportunities create value. Many companies try to minimize risk instead of maximizing value. Risk minimization can destroy value. We may have to change tack – Risk avoidance to Risk consciousness. The twin objectives of risk management are to manage risk and to be seen managing risk. It is all about actualities and perceptions.

The first step for bankers is risk identification. The next step is to priorities these risks after profiling them. Then come the 3M approaches of measuring, monitoring and managing risks. Banks need to reorganize and set-up risk management committees and project themselves as safe bets to the stakeholders.

The ongoing financial sector reforms have also brought about a major cohesiveness in the three markets – bank credit, money and security markets at the domestic level. The changed financial architecture has significant implications for corporate strategy, organization and performance necessitating a move for banks to become 'one-stop financial shops'.

The concept of risk refers to the degree of probability of the occurrence of an event that would disrupt the planned running of a process or operation. Once a particular or potential risk has been identified, it can be measured, and on the basis of that quantification, a strategy of risk management can be implemented. This concept of risk assessment and management works on the basis that not all risks can be completely eliminated. Indeed, given the cost of eliminating a risk and its probability, the management of risk means that some risks should be left as open risks.

One area where risk assessment and risk management is scrupulously employed is banking. The emphasis however has increasingly shifted towards an area of risk which is all encompassing-operational risk.

OPERATIONAL RISK

Operational risk is an area of risk that any reasonably complex enterprise will face, and is the risk wherein any systems, procedures, machinery or technology may cease to function adequately or even totally. It refers to the likelihood that these operating expenses vary significantly from what is anticipated, resulting in a decline in the net income and value of the company. The Basel Committee defines risk as "The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events." A new focus of the Basel II Accord is operational risk as per which a bank will be required to make capital allocations for operational risk from the year 2005. The shortcomings of banks made it imperative for them to protect themselves against the operational risks for the benefit of stakeholders and the constituents. From the perspective of capital adequacy, this risk covers technology risk, management/people oriented operational risks and legal risks.

Operation risk covers some of the key drivers of Basel II. These relate to technological advances leading to emergence of new financial products (through risk unbundling and rebundling) and new ways of delivering them (e-finance), progressively larger deregulation, particularly in emerging market economies, demographic changes and the nexus of increased competition, enhanced search for shareholder value and spread of financial safety nets.

These forces and their interactions have been reflected in securitization (commoditization of credit, and its associated risks and their sale and purchase in the marketplace), globalization and consolidation in the financial services industry. But Basel II Accord is an evolving process to handle financial innovation and increasing cross-border flows triggered by rapid technological advancements. Systemic reform of the banking system necessitates streamlined risk management, adequate capital provision, sound supervisory and regulatory practices, transparency and macroeconomic stability.

Banks and other financial players have been restructuring their working to circumvent regulations and meet the perceived demands of the customers' needs. Financial innovation of securitization and globalization and improved new technologies are nothing but extension of response by the financial institutions in the making of new products, consciously or otherwise. In addition to operational risk banks face financial risk. Finance being the core of banking business managing this risk becomes very vital for the industry.

FINANCIAL RISK

Assessing and measuring financial risk is the core business of the banking sector. Banks face financial risks in many forms. They are – Credit risk, Liquidity risk, Interest Rate risk, Market Risk and Foreign Exchange Risk.

Credit Risk occurs when a customer, who has been lent money, defaults.

Liquidity risk covers the possibilities when the patterns of banking activity may lead to a scenario wherein the bank simply does not have enough liquid funds to meet its liabilities at a given time.

Interest rate risk may arise when central bank interest rates may move away from where any given bank has assumed such rates will be for the purpose of setting rates for their own lending.

Market risk and foreign exchange risk are similar to interest rate risk in that market values and exchange rates may move out of line with expectations, and thereby underlying financial decisions.

Fundamentally, the major financial risk is the solvency risk, i.e., the bank may not have enough assets to meet its liabilities, and is measured in terms of available capital as against all risks. Financial risk management is, therefore, the process of assessing all the risks that a bank is exposed to, assume that all risks generate potential losses, and then work out a level of capital adequacy that a bank must maintain that will satisfactorily protect the bank from these risks.

In the past, risk was not given the kind of focus it is being given now. Most instruments had low leverage towards risks and consequently trading losses were less. Now, risk has become an integral part of any business. They are hedged by sophisticated tools. Increase of leverage in instruments has further complicated the risk management of banks because the same will have its effects on other risks such as credit risk, operational risk, etc. In this context banks/corporate have begun to seek for comprehensive solutions. This change in the way risk is managed is complimented by the regulators through corporate risk management systems, disclosures of risks, etc.

There is marked change in the total outlook of the financial institutions and more specially the banking industry with regard to their focus on the risk management systems as the same sounded good from the business point of view. This has influenced the changing attitudes in the risk taking by these companies and consequential risk management process. The companies started using new methods and new technologies. Even the corporate image and culture are redefined by these changes for enabling better procedural handling of risk factors.

Every financial institution is unique in its identity and composition of various features. Therefore, it is very difficult to implement any risk management strategy on sound lines. The unique features in each of the banks/financial institutions make it more difficult for uniform application of solutions.

Corporate Culture

A well-formulated risk management strategy in a bank is dependent upon some fundamental aspects of the company like the corporate culture, its procedures and technology. Any amount of regulatory intervention or force will not make the bank comply positively with regard to controlling of risks unless, their staff members themselves respond positively to the corporate needs and change their individual and collective outlook and attitude towards risk control and their decision making and cooperate in the corporate practices.

The Role of Procedures

Procedures including technology play a vital role in the execution and evaluation of a company's strategy towards risk management. Sometimes certain procedures will be followed out of sheer need and indispensability regardless of their effect on risk. Some practices are developed out of habit over a period of time and get established irrespective of their role in the management. Certain procedures empower the manpower at different strata. They need not be systemized codes or rulebooks. They can as well be directed to the activities and attitudes. The strength

of procedures depends on whether the unit/organization staff take those procedures in the right perspective with faith in their efficacy and the staff's responsibility and dedication to their individual and collective role. The importance of procedures and technology lies in formalizing the strategy of risk management. Lack of procedures will put the individual members in difficulty and there is ample probability of differences in opinions and decisions. Consequently, the making and implementation of such decisions are affected leading to the personal risk to managers and directors. A procedure is motivator and driving force for the efficacy and efficiency of machines and people respectively. Lines of reporting, trading authority and risk limits are certain examples in procedures. There is every need for periodical review and revision of procedures. Certain exigencies prompt contingent solutions for warding off the risks and there is every possibility of their becoming a risk factor in future if the same are habitually resorted to indiscriminately.

SYSTEMIC RISK

In recent years the financial sector, that includes in particular many central bankers, has become concerned with the concept and possibility of systemic risk in banking and financial markets. Systemic risk is the possibility that an entire system, such as international banking, may cease to function adequately or at all as a system. Systemic risk is therefore, a particularly serious (even catastrophic) risk because of its magnitude. The concern is that although systemic risk is clearly conceptually possible in banking, increased globalization and use of Over-the-Counter derivatives in modern banking meant that the risk of this possibility is markedly increasing. If that is indeed the case, the banking and financial sector must take very serious measures to understand systemic risk better and to attempt to manage this risk.

In 'Debt, Financial Fragility and Systemic Risk' E P Davis offers this definition of systemic risk: 'systemic risk', 'disorder', or 'instability' are used to describe a disturbance in financial markets which entail unanticipated changes in prices and quantities in credit or asset markets, which lead to a danger of failure of financial companies, thereby threatening to spread so as to disrupt the payments mechanisms and capacity of the financial system to allocate capital'.

Kaufman and Scott in 'What is Systemic Risk and Do Bank Regulators Retard or Contribute to it' define it thus: Systemic risk refers to the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by co-movements (correlation) among most or all of the parts. Thus, systemic risk is a particular risk in banking and financial markets because there is a strong interconnection between all the agents in the system. An inter-bank clearing market in itself establishes strong interrelations among the banks involved.

Further, investment banks will attempt to lay-off risk from major projects by packaging the debt and selling it to other investment banks and financial institutions. In addition, relatively recent developments in terms of banks using highly leveraged speculative derivatives, increases the severity of a risk to the whole sector from economic shocks. In this way, the banking and financial sector is inter-twined with strong and interdependent obligations and liabilities. The real risk of a bank suffering solvency risk is not the collapse of a bank, but the risk is that it will take many other banks with it, and ultimately bring the whole market down.

Kaufman and Scott identify three systemic risk scenarios in banking and financial markets.

- First, a macro-shock may cause a systemic risk of market collapse. A macro-shock is something of the order of an outbreak of war or a major environmental catastrophe. This may cause systematic collapse because it may actually justify it, but more likely it is the disruption to the availability of reliable and up-to-date information that makes rational decision-making difficult and a market herding panic inevitable. The relationship between the macro risk and the systematic collapse is, thus, one of direct causation. Such risks are relatively unlikely, and are, in practice, almost impossible to control through affordable risk management.
- The second form of systemic risk they identify is the 'domino effect' risk. This is a particularly severe risk in a system characterized by strong interdependence of agents. As the name suggests, the risk is that – one relatively minor event may set in a whole series of minor and major events that are unstoppable once started and cumulatively leave such an impact that it will collapse the system. Kaufman comments: 'It is the probability that cumulative losses will accrue from an event that sets in motion a series of successive losses along a chain of institutions or markets comprising a system. That is, systemic risk is the risk of a chain reaction of falling interconnected dominoes'. Thus, for example, one bank may go insolvent owing a significant sum to another bank, but it is severe enough to push the latter bank into insolvency as it owes a significant sum to another bank, and so on. This is a very severe systemic risk where there are strong networks of financial cross-liabilities and cross-holdings between institutions in a system. It is similar to a macro shock risk in that there is an element of direct causation, where one insolvency directly causes a whole 'domino fall' chain. However, it differs from a macro shock in that there is a particular correlation amongst the agents that are directly affected, though the end result of system collapse will be often the same.
- The third form of systemic risk is 'contagion' risk. Again, like the 'domino effect' the risk in a system is that relatively minor event initially may go on to have serious spill over effects. However, in contagion risk what is seen is systems breakdown through the gradual and chaotic spread of a disturbance via often indirect connections. It is the sort of risk that demonstrates correlation, often through only indirect causation. Kaufman and Scott comment that it emphasizes similarities in third party risk exposures among companies involved. When one unit experiences an adverse shock from, say, the failure of a large financial or non-financial company that generates severe losses, uncertainty is created about the values of other units potentially subject to the same shock. Therefore, such a contagion system risk can, if the contagion is serious enough, cause a system collapse through correlation and causation meshing as a 'domino' risk.

However, what may be more significant in contagion risk is that the system reacts to the contagion disproportionally. The contagion event causes not just agents in the system to become directly exposed to a known fanning out of losses, but causes those agents to re-evaluate, and more specifically doubt the quality of the information they possess on other agents and the market. For example, if one bank collapses through losses to a defaulter country, the entire banking sector looks risky until it can be established that no one else has large exposures to the defaulting country. It is precisely this period of doubt that must be considered as a systemic risk, because the spread of a general doubt in the strength of a system may itself perversely precipitate that very collapse. The particular problem is that in this contagion even sound and reliable agents will also be effectively damaged, perhaps fatally, just as the guilty and unreliable agents.

RISK LIMITATION

Before studying the response from the industry for risk we shall discuss in brief what risk limitation in a bank is all about.

Risk limitation is a part of risk management. In order to limit a risk, the bank should first find what amount of risk it can absorb. In other words, it is called the bank's risk capacity or the maximum unforeseen loss that the banking company could suffer and still manage to keep itself afloat. The overall limit set for the bank will be divided among the different segments and clients keeping their size and features in mind. Any calculation in this direction will necessarily take into consideration the bank's properly valuated reserves, which were set specifically for the purpose of covering the unexpected. In practice, not all risks can be quantified and at the same time not all risk-saving expenses can be estimated and justified. The bank should endeavor towards balancing the actual data versus the planned data using the right techniques of measuring and quantifying the risks on uniform basis.

It is to be understood that in the complex and multifaceted management process of risk management, the element of risk-taking is an integral part. This process requires continuous planning, supervision, review and revision as per the needs of the time.

Throughout the consolidation phase of 1990's, banks relied on three primary strategies to create shareholder value. They are:

- Risk reduction – Securitizing a greater number of the loans they originated, as well as other assets sitting on their books.
- Revenue diversification – Expanding their revenue base through additional sources of non-interest income.
- Consolidation – Capturing economies of scale and scope through acquisitions and mergers.

Although initial results were impressive, the returns from these strategies have now flattened – and a few undesirable consequences have emerged. Alleviating risk through the sale or securitization of assets had the unpleasant side effect of putting even more distance between banks and their customers. Further growth in fee-related income through the introduction of service charges worked against the need to cultivate customer loyalty. And a decade full of mergers and acquisitions left banks with organizational, process and system complexity, which placed enormous strain on operational efficiency and financial performance.

With all these changes, banks are still largely operating with the same traditional business structures where distribution occurs through product silo and operations are biased toward internally manufactured products. Within this structure, even leading banks cannot seem to squeeze out any more cost, and customers generally see very little or no differentiation among banks. Given their financial challenges, banks cannot afford to have capabilities duplicated across product silos, with each product operating its own processes, systems and product-specific channels. And although they offered increased efficiency, vertically integrated supply chains limited customer choice, leaving companies with an undifferentiated value proposition and lower overall customer wallet share. It's no surprise that banks are moving away from the confines of their historical business structures. But with value continuously shifting to different parts of the value chain, many banks are struggling, unsure which areas of their business matter most and also uncertain where they are heading. With the dynamics of the future unclear, it only makes it more apparent that banks will need:

Greater focus on what differentiates them from the competition, less attention – and spending – on commodity-like functions.

Heightened responsiveness to ongoing changes in the marketplace, more empowered customers and increasingly complex demands from regulators and stakeholders.

Variable cost structures that allow banks to accommodate fluctuations in market demand and product preferences while improving financial position through lower cost structures.

Improved resilience to counteract increased internal and external uncertainty and marketplace volatility – whether protecting your business from shocks such as natural disasters, privacy and security threats and geopolitical events or addressing everyday challenges like business expansion and credit risk.

The question is: How will banks reach that enviable position? Two primary paths seem clear – one involves the industry as a whole and the other is traveled by individual banks. As an industry, banking is moving away from a set of independent, vertically integrated institutions toward a network of affiliated financial institutions. At the same time, individual enterprises are reconstructing– breaking product silos into small, encapsulated business components that can be shared across the enterprise.

In fact, the confluence of these two paths is propelling banks toward an on-demand operating environment where a bank's business structure and supporting business processes become flexible enough to respond rapidly to virtually any customer demand, market opportunity or external threat.

Box 2: The Enterprise-wide Approach to Risk Management Strategies for Weathering the Corporate Storm

The calculation of risk has always been central to managerial decision-making, but today executives are acutely aware of the need to deal proactively with uncertainties that can threaten their business.

Risks are often closely connected. Operational risks, for example, can quickly evolve into market risks if word gets out and the share price falls.

The regularity of such incidents along with high-profile corporate scandals – such as those happened at Barings Bank, Enron and Worldcom – provoked a response from regulatory bodies throughout the 1980s and 1990s.

The Basel Committee for Banking Supervision, the Europe-based regulatory body, and the UK's Turnbull Committee now recommended corporations and financial institutions to adopt a more thoroughgoing approach to risk management, otherwise known as Enterprise Risk Management (ERM).

ERM is a systematic way of understanding and managing the various risks a company faces. How is it carried out? First, managers must identify business risks the company faces at all levels, from the Board of Directors to line managers.

This may not be as straightforward as it seems because people tolerate different levels of risk within each company.

Also, while an ERM framework offers the prospect of a transparent and consistent language of risk throughout organizations, most companies have yet to speak such a language. A May 2002, survey of executives by McKinsey revealed that 36 percent did not fully understand the risks that their businesses facing.

While identifying the risks, managers should consider three broad categories. First, financial risks can be created by market fluctuations or changes in the status of the company's creditors.

There are methods for reducing such errors.

Manufacturers such as General Electric have initiated programs such as Six Sigma, which aim to reduce the number of errors radically in a given production cycle.

Businesses are exposed to business-volume risk when they suffer unexpected changes in the demand for their products and services, their supply structure or the competitive environment.

The second step in ERM is the assessment of risk. Advanced techniques in risk modelling - such as decision analysis, Value-at-Risk calculations and scenario planning - allow managers to gauge the likelihood of certain events.

The final step is the most crucial: once risks are identified and evaluated, they must be managed. There are typically two options here – using internal resources, such as self-insurance, or transferring risk and sharing it with another party.

Managers can also bundle together different types of risk and trade these with other parties. In 1997, for instance, the technology company Honeywell took out an insurance policy that bundled property and liability risks against currency risks. The initiative helped the company cut down its risk management costs by more than 15 percent.

A well-managed ERM policy encourages a common language of risk among board members, managers, suppliers, customers, investors and so on. It helps people at the front line - who spot warning signals of potential problems - to communicate them more quickly to those who can decide to take evasive action.

ERM does not impose a centralized decision-making process for risk management. On the contrary, it is designed to increase accountability for risk in each and every business unit.

What does it take to put an ERM policy into place? First, no risk-related initiative can be launched without high-profile commitment from senior managers. This might mean regularly communicating on risks with employees and outsiders, such as investors or suppliers.

Second, risk awareness must be part of the corporate culture. The question is how can you achieve this? One answer is to appoint a Chief Risk Officer (CRO), whose prime function is to make risk management a central part of the business.

ERM often exposes unforeseen risks to the company and challenges managers to look for enterprise-wide solutions. Done well, it frees up company resources and capital reserves for activities that can raise shareholder value.

Integrating risk management into day-to-day operations, rather than letting employees react to risks as they crop up, makes it a source of competitive advantage.

Source: Ayse Onculer, London, September 02, 2001, Business Standard.

IT IMPLEMENTATION CHALLENGES

Although product and service silos still have a stronghold within most financial services institutions, the monolithic view of the enterprise is fading, as is vertical integration. Whether of their own volition or spurred by new players arriving on the scene with significantly improved value propositions for particular parts of the value chain, companies are beginning to specialize. They are selecting a more specific industry role – manufacturing, distribution, risk management or processing – that suits their strengths and turning externally (or internally to other business units besides their own) to supplement weak capabilities.

In most financial services industries, the shift from vertical integration to a networked structure usually begins with distribution as companies seek additional outlets for their manufactured product. The banking industry is no exception to this trend. More and more banks are moving towards total branch computerization and anywhere and anytime banking.

Although the role of information technology in cutting costs and boosting productivity has been well documented yet, the link between IT and risk management has not been properly developed. As the complexity of transactions increases, people find it difficult to understand and monitor the risk involved. A good IT infrastructure is required besides other needs, to make information available on a timely basis so that the senior management can take stock of the situation and frame suitable risk management strategies. In fact, by not investing in information systems, a bank could be assuming major risk.

Box 3: Information Technology (IT) Risk in Banks

Banking is a business which is full of risks. Lot of attention is given to credit and market risk by banks ignoring operational risks. Operational risk is because of failure of man, machine or systems to operate as expected. With more and more implementation of Information Technology based systems, the chances of IT related operational risks have increased day by day, unless some measures are not implemented. Banks have to identify the risks from the increased usage of computerization and automation in their processes as the types of controls required to manage the risks are different form the manual systems.

Nature of IT Risks

The IT risks can be classified under (a) IT environment risks, (b) IT operations risks and (c) product/service risks.

a. IT Environment Risk – Regulatory Risk, Strategic Risk, Organization Risk, Location Risk and Outsourcing Risk arise due to the commercial and business environment within which the computer and telecommunication systems are operating:

   i. Regulatory Risk – Regulatory breaches can result in diminishing reputation, increased cost of capital, limited business opportunities and punitive action, which banking operations may ultimately end up in loss.

   ii. Strategic Risk – The bank may not be able to achieve its effectiveness and loose competitive edge and may place too much pressure on the bank's IT resources to adapt to new business environment, as new products and services come on-line when a bank adopts inappropriate IT strategies.

   iii. Organization Risk – When the organizational structure fails to provide and define reporting lines and responsibilities for the IT functions, it can lead to misunderstanding of responsibility and a poor distribution of human and financial resources.

   iv. Location Risk – Depending on the location of a bank's data processing activities it can be susceptible to natural events such as floods, earthquakes, storms and other events like riots or sabotage.

   v. Outsourcing Risk – The responsibilities and liabilities of vendor and client may not be clear without proper management control and documentation. Over reliance on single vendor/supplier increases the risks from their failure and may lead to unacceptably high costs.

b. IT Operations Risk – Error Risk, Computer Fraud Risk, Disclosure Risk and Interruption Risk are the risks, which arise from transaction processing on computer systems.

   i. Error Risk – Errors may affect the completeness and may end up resulting loss to the bank, which are made during the development and modification of computer programs simple error in data entry or misuse of some tools.

   ii. Computer Fraud Risk – The risk is due to the ease with which the fraudsters hide their actions in the system especially during times of business and system change. Such risks are more likely when the security and control systems are weak or not properly implemented.

   iii. Disclosure Risk – Information passed on communication network includes very sensitive and financial and other data of customers. Bank can have negative impact and reputation if the information is disclosed intentionally or accidentally and may loose its customers.

   iv. Interruption Risk – The failure of discontinuity of computer operations may lead to interruption to the bank's operations and customer's dissatisfaction and loss of business. If the computer related infrastructures are not secured there will be much impact on the business continuity.

c. Product/Service Risk – The services offered by banks like Automated Teller Machines (ATMs), Electronic Funds Transfer (EFT), etc. are required to be available to the customers without any disruption. The operational risks associated with these products remain fundamentally unchanged. The way in which management design and implement a control framework to mitigate these risks is different to manual processes.

Source: www.rbi.org.in

Since only a few large companies will be able to span the full range of products in a vertically integrated manner, most companies will focus exclusively on areas where they have comparative advantage. Distributors will own the customer interface, while specialists with deep product expertise will develop new products based on segment-specific customer insights that the distributors provide. Companies will take advantage of scale efficiencies offered by selected processors – perhaps even tapping into low-cost labor pools overseas.

Most critical of all, the customer too benefits. With access to best-of-breed products through a variety of distributors and improved customer service, customers are no longer forced to choose between seamless service and a superior product. As additional businesses start to deconstruct and bank revenues shift, banks will need to leverage their biggest asset: their customer base. In order to do this, banks will have to revisit their current business structures, looking to capitalize on hidden efficiencies and leverage customer relationships across their enterprises.

Risk management lies at the core of the bank's business strategy. It is wrong to view risk management as a field which deals with credit risk, interest rate or exchange rate movements. Rather, risk management is all about reducing vulnerability by making sure that cash is consistently available to make value adding investments and providing the stakeholder the best possible returns.

SUMMARY

- Banks in India had to change the old ways of doing business due to factors such as technological advancements, disintermediation pressures arising from a liberalized financial marketplace, increased emphasis on shareholder value, and macroeconomic pressures and banking crises after globalization in the 1990s. Consequently, banks and other financial institutions were compelled to adopt comprehensive risk management practices, due to the ever-increasing competition as well as stringent regulatory norms.
- Risk assessment and management works on the basis that all risks cannot be completely eliminated. Indeed, given the cost of eliminating a risk and its indispensability, the management of risk means that some risks should be left as open risks. Banks face two major types of risk – operational risk and financial risk. Every bank is unique in its identity and composition making it difficult for implementing any uniform risk management strategies.
- A well-formulated risk management strategy in a bank is dependent on some fundamental aspects like the corporate culture, procedures and technology. The importance of procedures and technology lies in how successful they are in formalizing risk management.
- Risk limitation is part of risk management. The bank should first find what amount of risk it can absorb in order to limit its risk exposure.
- Risk reduction, revenue and diversification are three key primary strategies banks rely on to create shareholder value.

Glossary

Accounting Information Systems : Systems that record and report business transactions, the flow of funds through an organization, and produce financial statements. This provides information for the planning and control of business operations, as well as for legal and historical record-keeping.

Acid Test Ratio : A liquidity measure which is defined as: (Current Assets – Inventories)/Current Liabilities.

Acid-Test Ratio : One of three ratios commonly used to evaluate a firm's liquidity; calculated by dividing cash by current liabilities.

Activity Based Costing (ABC) : A form of cost accounting that focuses on the costs of performing specific functions (processes, activities, tasks, etc.) rather than on the costs of organizational units. ABC generates more accurate cost and performance information related to specific products and services than is available to managers through traditional cost accounting approaches.

ALCO : Is the acronym for Asset and Liability Committee. Term used frequently in banking industry.

American Bankers Association (ABA) : An organization of commercial banks, founded in 1875 to keep members aware of developments affecting the industry, to develop educated and competent bank personnel, and to seek improvements in bank management and service.

American Exercise : A provision that permits exercise of an option any time prior to expiration.

Analog Computer : A computer that operates on data by measuring changes in continuous variables like voltage, pressure and resistance.

Analysis of Variance (ANOVA) : A calculation procedure to allocate the amount of variation in a process and determine if it is significant or is caused by random noise. A balanced ANOVA has equal numbers of measurements in each group/column. In a stacked ANOVA each factor has data in one column only and so does the response.

Application Service Provider (ASP) : Is a company that offers individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers.

Application Software : Programs that specify the information processing activities required for the completion of specific tasks of computer users. Examples are electronic spreadsheet and word processing programs or inventory or payroll programs.

Arbitrage-Free Pricing : The approach to pricing instruments that underlies essentially all of financial engineering.

ARCH : Auto Regressive Conditional Heteroskedasticity

Artificial Intelligence (AI) : A science and technology whose goal is to develop computers that can think, as well as see, hear, walk, talk, and feel. A major thrust is the development of computer functions normally associated with human intelligence, for example, reasoning, inference, learning, and problem solving.

Asset Turnover : A ratio used to evaluate the profitability of a firm; net sales in a given period are divided by total assets.

Audit Trail : The presence of media and procedures that allow a transaction to be traced through all stages of information processing, beginning with its appearance on a source document and ending with its transformation into information on a final output document.

Back Office Operations : The part of a firm that is responsible for post-trade activities. Depending upon the organizational structure of the firm, the back office can be a single department or multiple units (such as documentation, risk management, accounting or settlements). Some firms have combined a portion of these responsibilities usually found in the back office, particularly those related to risk management, into what they term as middle office function.

Balance of Trade : The difference between the value of the goods and services sold to foreign nations (exports) and the value of the goods and services bought from foreign nations (imports) in a given period.

Bank Collection Float : The time that elapses between when a check is deposited into a bank account and when the funds are available to the depositor, during which period the bank is collecting payment from the payer's bank.

Bank Rate : The rate at which a country's central bank will make short-term loans to chartered banks and other financial institutions, and against which the benchmark for prime rates is set by financial institutions.

BANKNET : A communication software to provide message and file transfer between branches of banks and across banks

Base Currency : The currency in which a VaR measure quantifies market risk.

Basket Option : An option on a portfolio or "basket" of underliers.

Basle Committee : An international committee that has played a leading role in standardizing bank regulations across jurisdictions.

Basle II : An international accord on bank capital requirements to replace the earlier 1988 Basle Accord.

Batch Processing : A category of data processing in which data are accumulated into batches and processed periodically.

Benchmarking : Benchmarking is an improvement tool whereby a company measures its performance or process against other companies' best practices, determines how those companies achieved their performance levels, and uses the information to improve its own performance.

Bid-ask Spread : The difference between prices at which dealers are willing to buy or sell.

Black (1976) Option Pricing Formula : A pricing formula for European options on commodities, forwards or futures.

Black-Scholes (1973) Option Pricing Formula : The original option pricing formula published by Black and Scholes in their landmark (1973) paper. Used to price European options on non-dividend-paying stocks.

Black-Scholes Theory : Another name for option pricing theory.

Book Entry System : An accounting system that permits the transfer of claims (e.g. electronic transfer of securities) without the physical movement of paper documents or certificates.

Brainstorming : A Strategic Planning process and Risk Assessment tool that attempts to unlock the imagination of a group by stimulating a "storm" of ideas through a structured process.

Business Process Outsourcing : Business Process Outsourcing (BPO) is the contracting of a specific business task, such as payroll, to a third-party service provider.

Callable Bond : A bond which allows the issuer to repurchase the bond for a specified price on certain dates prior to the bond's maturity.

CAMELS Rating System : An international bank rating system with which bank supervisory authorities rate institutions according to six factors. The six areas examined are represented by the acronym "CAMELS." The six factors examined are as follows:

C – Capital Adequacy

A – Asset Quality

M – Management Quality

E – Earnings

L – Liquidity

S – Sensitivity to market risk.

Capital Allocation : A process of choosing what ventures, deals or trades to engage in, usually based upon some cost or risk-return analysis.

Cash Flow Management : Provides better management and forecasting of cash flow through a host of services such as electronic file transfer for bulk payments/collections, liquidity management, etc.

Cash Management Services : Cash management can generally be defined as the efficient utilization of cash through coordinated management of payments, collections and cash balances. The objectives are to reduce costs, enhance control and optimize returns.

CAT Standards : A set of standards for the charges, access and terms relative to a particular financial product, such as Individual Savings Accounts (ISAs), devised by the Government to compare products from different providers.

CBO : Collateralized Bond Obligation.

Central Bank : The principal monetary authority of a nation, a central bank performs several key functions, including issuing currency and regulating the supply of credit in the economy. The RBI is the central bank of India.

Central Processing Unit : Central Processing Unit (CPU) is a microscopic circuitry that serves as the main information processor in a computer.

CHAPS (Clearing House Automated Payment System) : An electronic transfer system for sending same day value payments from bank to bank.

CLO : Collateralized Loan Obligation. See CDO.

Commodity Futures Trading Commission : The regulator of futures and options exchanges in the United States.

Computer-Aided Design/Computer-Aided Manufacturing (CAD/CAM) : The use of computer systems with advanced graphics hardware and software to support engineering design and to convert CAD drawings into finished products with little human intervention.

Consumer Credit : Loans for personal or household use as opposed to business or commercial lending. Loans are generally unsecured, not backed by collateral.

Cost/Benefit Analysis : Identifying and analyzing the benefits and costs of a proposed system.

Cost/Benefit Analysis : A Risk Management tool used to make decisions about Accepting Risk or using some other risk management technique.

Covariance : A parameter, related to correlation, that indicates the tendency for two random variables to "move together" of "co-vary."

Covariance Matrix : A symmetric matrix indicating all the covariances and variances of a random vector.

Credit Default Swap : A type of credit derivative. A Swap in which A pays B the periodic fee, and B pays A the floating payment that depends on whether a predefined credit even has occurred, or not. The fee might be quarterly, semiannual, or annual. The floating payment would likely occur only once, and might be proportional to the discount of the reference loan below par. The credit event might be a declaration of bankruptcy or violation of a bond indenture or loan agreement.

Credit Derivative : A derivative instrument designed to transfer credit risk from one party to another.

Credit Distress : A firm can have many types of credit obligations outstanding. These may be of all manner of seniority, security and instrument type. In bankruptcy proceeding, it is not uncommon for different obligations to realize different recovery rates including perhaps 100% recovery – zero loss. It is the obligor that encounters credit distress carrying all of his obligations with him. Thus, individual obligations will be exposed to credit distress even though some may not realize an actual default (i.e., some may have zero loss).

Credit Enhancement : Any methodology that reduces the credit risk of a transaction with a counterparty.

Credit Exposure : The potential for loss in the event of a default.

Credit Linked Note : A type of credit derivative.

Creditworthiness : A creditor's measure of a consumer's past and future ability and willingness to repay debts.

Cross-Selling : Selling by a salesperson of some part of the company's total product range for which another division or salesperson has prime responsibility.

Cryptography : It is the science of using mathematics to encrypt and decrypt information.

Data Mining : This refers to the process of finding relevant information for enhancing knowledge. It attempts to discover statistical rules and patterns automatically from data.

Data Warehousing : A system that stores, retrieves, manages, or otherwise manipulates massive amounts of data that may be from the organization's databases and external sources. The warehouse of data is often separated from the organization's production databases, so that users can use this resource without reducing the response time for an organization's routine data processing operations.

Database Administration : A data resource management function that includes responsibility for developing and maintaining the organization's data dictionary, designing and monitoring the performance of databases and enforcing standards for database use and security.

Database Management System (DBMS) : A set of computer programs that controls the creation, maintenance, and utilization of the databases of an organization.

Debit Transfer System : A funds transfer system in which debit collection orders made or authorized by the payer move from (the bank of) the payee to (the bank of) the payer and result in a charge (debit) to the account of the payer; for example, cheque-based systems are typical debit transfer systems. Also called debit collection system.

Decision Support Systems (DSS) : An information system that utilizes decision models, a database, and a decision maker's own insights in an *ad hoc*, interactive analytical modeling process to reach a specific decision by a specific decision-maker.

Default Risk : Also referred to as credit risk (as gauged by commercial rating companies), the risk that an issuer of a bond may be unable to make timely principal and interest payments.

Delta : The Greek factor sensitivities measuring a portfolio's first order (linear) sensitivity to the value of an underlier.

Derivatives : Financial instruments or contracts which are valued based on (derived from) the value of other financial instruments. This is a financial Risk Financing strategy. These financial instruments can be highly Leveraged and therefore highly Volatile. A common form of derivative is a foreign currency hedge contract to finance overseas trade: the purchase of an option to buy or sell a foreign currency at a certain date for a certain price. This Hedging example reduces the risk of future price fluctuations by trading an uncertain price in the future for a certain (guaranteed) price now, for a fee.

Derivatives Pricing Theory : The body of financial theory used by financial engineers to value derivative instruments.

DFSS : Design for Six Sigma (DFSS) is a systematic methodology utilizing tools, training and measurements to enable us to design products and processes that meet customer expectations and can be produced at Six Sigma quality levels.

DMAIC : Define, Measure, Analyze, Improve and Control (DMAIC) is a process for continued improvement. It is systematic, scientific and fact based. This closed-loop process eliminates unproductive steps, often focuses on new measurements, and applies technology for improvement.

Dual Remapping : A type of remapping used in Value-at-Risk measures.

Dynamic Hedging : A strategy that involves rebalancing hedge positions as market conditions change; a strategy that seeks to insure the value of a portfolio using a synthetic put option.

Economic Capital : Capital employed in internal capital allocation as a proxy for a firm's ability to take risk in exposures.

Electronic Banking : Any banking activity which can be accessed through electronic means such as ATMs, automated call centers, personal computers, transfer funds, buy and sell shares, etc.

Electronic Commerce : E-commerce, or electronic commerce, is conducting business communications and transactions via computers over networks. It is the buying and selling of goods and services through digital communication.

Electronic Data Interchange(EDI) : The direct exchange of information electronically, from one firm's computer to another firm's computer in a structured format.

Electronic Data Capture : Process used for capturing and transferring the encoded information on the magnetic strip from a bank card or debit card at the Point-of-Sale (POS) to the processor's database.

Enterprise Resource Planning : An amalgamation of a company's information systems designed to bind more closely to a variety of company functions including human resources, inventories and financials while simultaneously linking the company to customers and vendors.

Enterprise Risk Management : The extension of financial risk management to non-financial risks.

E-Treasury : E-treasury is a next generation universal integrated banking system with a modern architecture. It supports forex and domestic treasury operations in multi-currency, multi-branch environment.

Euro Interbank Offered Rate : Refers to indicative short-term interest rates available for the Euro.

Exchange Rate Mechanism (ERM) : The methodology by which members of the EMS maintain their currency exchange rates within an agreed-upon range with respect to other member countries.

Ex-Dock : A method for settling physical commodity trades.

Executive Information Systems (EIS) : An information system that provides strategic information tailored to the needs of top management.

Exotic Derivative : A complicated or specialized derivative instrument.

FBO : For Benefit Of (FBO) is used in electronic funds transfers to nominate a second beneficiary or to designate a contact person or organization.

Feasibility Study : A preliminary study that investigates the information needs of the users and the objectives, requirements, cost/benefits and feasibility of the proposed system.

Federal Reserve : The central bank of the United States.

FEDI : Financial Electronic Data Interchange (FEDI) involves the computer to computer transmission of both payment instructions and remittance details using international message standards. An example would be trade payments, for example, a retailer sending a payment to a supplier in payment of multiple invoices.

Fedwire : Payment system operated by the Federal Reserve/Payment mode: transactions that are electronically initiated and settled on the same day.

File Transfer Protocol (FTP) : A standard way of transferring files from one computer to another on the Internet.

Financial Risk Management : Practices by which a firm optimizes the manner in which it takes financial risk.

Financial Services Modernization Act of 1999 : The US legislation that revoked the Glass-Steagal separation of investment and commercial banking.

Firewall : Protection systems that monitor all Internet or external communications activity at a site. It closes all connection attempts from unauthorized users. May provide activity logs to identify intruders, examine programs and files as they are downloaded for virus and to ensure that users downloading files and programs have the authority to do so.

Fixed Exchange Rate System : A system in which the values of various countries' currencies are tied to one major currency such as US dollar, gold, or special drawing rights.

Floating Exchange Rate System : A system in which the values of various currencies related to each other are established by the forces of supply and demand in the market without intervention by the governments involved. In practice, most floating rates are really "managed float" with periodic *ad hoc* intervention by central banks.

Foreign Currency Fixed Deposit : A FCTD is a fixed term investment denominated in a foreign currency that is available to both individuals and businesses.

Franchising : An arrangement in which a supplier grants a dealer the right to sell a product in return for some percentage of the total sales; typically, the supplier provides buildings and equipment, management advice and marketing assistance to the franchisee, who agrees to operate according to the franchisor's general rules.

GARP : Coopers and Lybrand's Generally Accepted Risk Principles for financial services institutions.

Government Bond : Debt obligations of the US government, consisting of Treasury bills, notes and bonds, and carrying the highest credit rate possible. Also referred to as government securities.

Gross Settlement System : Primarily represent a bank's obligation to make payments to third parties on behalf of its clients if its clients are unable to make the required payments or meet other contractual requirements.

Historical VaR : A category of VaR measures that employ an historical transformation.

Indian Financial Network (INFINET) : The INFINET is primarily a TCP/IP based network. It is a Closed User Group (CUG) Network and uses a blend of communication technologies such as VSATs and Terrestrial Leased Lines.

Inflation Risk : The risk that the value of assets or income from investments will be less in the future as inflation decreases the value of money. As inflation increases, the value of a Fund's assets, and the value of the Fund's distributions, can decline.

Initial Margin : An amount of money that must be on deposit with a broker before you can put on a futures position.

Institute for Development & Research in Banking Technology (IDRBT)	:	Established by the RBI in 1996 as an autonomous centre for Development and Research in Banking Technology at Hyderabad.
Integrated Risk Management	:	The consideration of Risk at all levels of the organization, from the Strategic to the day-to-day job of the customer-facing employee. Integrating risk management into internal auditing means adopting Risk-Based Auditing and using risk management tools to plan internal audits.
Integrated Services Digital Network (ISDN)	:	A technology that uses existing common carrier lines to simultaneously transmit voice, video, and image data in digital form.
Interest Rate Policy	:	An arbitrage condition that must hold between the spot interest rates of different currencies.
Interest Rate Risk	:	The potential impact on the bank's earnings and economic value due to changes in interest rates. Rising interest rates could, for example, increase funding costs and reduce the net interest margin earned on a fixed yield mortgage portfolio.
Interest Rate Swap	:	Used to alter the cash flow characteristics of an institution's assets so as to provide a better match with its liabilities.
Internal Capital Allocation	:	A process intended to ensure that an organization engages in transactions that are – usually from a risk-return standpoint – most desirable.
International Banking	:	A sub-set commercial banking transactions and activity having a cross-border and/or cross currency element.
Internet	:	The Internet is the world's largest computer network. It is a collection of interconnected networks all freely exchanging information.
In-the-money	:	A condition, where, an option has a positive intrinsic value.
Intranet	:	An intranet is an internal corporate network built using Internet and World Wide Web standards and products. It is used by the employees of the organization to gain access to corporate information.
Intrinsic Value	:	The component of an option's market value that could be realized by exercising the option immediately.
ISDN	:	Integrated Systems Digital Networking (ISDN). A hierarchy of digital switching and transmission systems that provides voice, data, and image in a unified manner. ISDN is synchronized so that all digital elements communicate in the same protocol at the same speed.
ISO 9000	:	A series of quality assurance standards designed by the International Organization for Standardization (ISO) to ensure consistent product quality under many conditions.
Junk Bond	:	A bond whose credit rating is below BBB.

Just-In-Time (JIT) : Just-In-Time (JIT) refers to ordering goods or products so they arrive just-in-time for you to use them. This reduces the costs of storing excess and unwanted stock.

KMV Model : A commercial implementation of the asset value model of credit risk.

Letter of Credit : A negotiable instrument issued by bank that guarantees payment by the bank on behalf of the bank's customer. Common terms are standby letter of credit and documentary letter of credit. A standby letter of credit is typically designed to be payable to the holder, also known as the beneficiary, if the applicant, usually the bank's customer, does not perform on some pre-arranged agreement. Standby letters of credit are generally used domestically. Documentary letters of credit are generally expected to be collected upon as a form of collection between parties doing business who are unfamiliar with each other and the vendor or supplier is unable or unwilling to provide terms. Documentary letters of credit are generally used internationally. Letters of credit can also be converted in to a Banker's Acceptance.

Leverage : Debt financing or anything that can similarly magnify the risk and reward of an investment.

Libor : London Interbank Offered Rate.

Linear Remapping : A global remapping that replaces a portfolio mapping function with a linear polynomial.

Linear Transformation : In the context of Value-at-Risk, a transformation procedure applicable to linear portfolios.

Local Area Network (LAN) : An interconnected group of intelligent microcomputers or terminals within a small geographic location.

Long-short Position : A position that is long one asset and short another.

LRAM : The Livermore Risk Analysis Methodology developed by Charles Cresson Wood using both control failure and Vulnerability Analysis to generate Risk Scenarios.

Mainframe : A large-size computer system, typically with a separate central processing unit, as distinguished from microcomputer and mini computer systems.

Management Information System (MIS) : A management support system that produces pre-specified reports, displays, and responses on a periodic, exception, or demand basis.

Margin Call : A demand for additional margin.

Market Exposure : For market-driven instruments, there is an amount at risk to default only when the contract is in-the-money (i.e., when the replacement cost of the contract exceeds the origination value). The exposure/uncertainty is captured by calculating the netted mean and standard deviation of exposure(s).

Market Neutral : Having balanced long and short positions resulting in no net exposure to broad market moves.

Market Penetration	:	A growth strategy in which a company concentrates its efforts on its target market in order to attract a higher percentage of users of its product.
Market Penetration Pricing	:	An approach to pricing in which a manufacturer sets a relatively low price for a product during the introductory stage of its life cycle with the intention of building market share. See, *Market Skimming Pricing.*
Market Portfolio	:	A theoretical portfolio which comprises all risky assets available to investors.
Market Risk	:	Exposure to the uncertain market value of a portfolio.
Market Value	:	A valuation assigned to an asset based on the price it might fetch in the market.
Mark-to-Market	:	The act of assigning a market value to an asset.
Mark-to-Market Exposure	:	Credit exposure calculated from instruments' current market values.
Mark-to-Market Mode	:	A mode of analysis for a portfolio credit risk model.
Modem or Modulator/Demodulator	:	A communications device that converts signals from analog to digital and vice versa.
Modern Portfolio Theory	:	A body of theory relating to how investors optimize portfolio selections.
Mortgage-Backed Security	:	A security interest in mortgage collateral.
Multitasking	:	The concurrent use of one single computer to accomplish several information processing tasks.
NASD	:	National Association of Securities Dealers.
Netting	:	The offsetting of cash flows or other obligations against each other.
New Account Conversion Ratio	:	A measure used to evaluate a salespeople in which the conversion rate of prospects to customers is calculated.
New Product Development	:	The creation of new products needed for growth or to replace those in the decline stage of their life cycle; the stages in the new product development process are commonly listed as idea generation; screening; concept development and testing; the formulation of marketing strategies; business analysis; production; market testing; and commercialization.
Niche Banks	:	Smaller banks that cater to particular communities or certain industries. These banks have been thriving in the fallout from mega-bank mergers.
Non-linear Derivative	:	A derivative instrument whose payoff diagram in highly non-linear.
NSF	:	Also referred to as a returned or "bounced" cheque charge or non-sufficient funds fee. The amount of money charged to an account holder whose account has insufficient funds available to pay the cheque, which is returned to the party who cashed it unpaid. (The bank did not advance the funds to cover cheque.)

Offshore Banking : A reference to financial operations transacted outside the country in question. An offshore bank is a bank located outside the country of residence of the depositor, typically in a low tax jurisdiction that provides financial and legal advantages.

Online Analytical Processing (OLAP) : It designates a category of applications and technologies that allow the collection, storage and reproduction of multidimensional data.

Option Pricing Theory : The body of financial theory used by financial engineers to value options and other derivative instruments.

Out-of-the-money : A condition, where, an option is neither at-the-money nor has any intrinsic value.

Over-the-Counter : Traded in some context other than a formal exchange.

PIN : This stands for personal identification number. It is a secret number given to an account holder to be used when they put their credit card or cash card into an Automatic Teller Machine (ATM). If the number they use is correct they will be allowed to access their account.

Portfolio Mapping : A functional relationship specified by a VaR measure between a portfolio's value and the key vector.

Portfolio Theory : A body of theory relating to how investors optimize portfolio selections.

Pre-settlement Risk : Credit risk of default on a derivative instrument prior to final settlement.

Protocol : A set of rules and procedures for the control of communications in a communications network.

Random Access Memory (RAM) : A type of memory in which data is stored in addressable locations so that the data can be accessed directly without having to move sequentially through all the data stored; random access memory is volatile.

Read-only Memory (ROM) : Computer memory that can only be read, not written to or changed. Program stored in ROM are not lost when power is shut-off.

Real Time Processing : Pertaining to the performance of data processing during the actual time a business or physical process transpires, in order that results of the data processing can be used to support the completion of the process.

Replacement Cost : The cost of replacing an obligation of a counterparty.

Replacement Risk : The consequence of settlement risk. If you have not received payment from your counter party, you now have to enter the market and make the necessary purchase/sale to settle your books thus exposing your firm to the prevailing market rates.

REPO Rate : The rate of interest on a general collateral REPO transaction.

Repurchase Agreement : An agreement to sell and subsequently repurchase a security.

Retail Banking	:	Retail banking is typical mass-market banking where individual customers use local branches of larger commercial banks. Services offered include: savings and checking accounts, mortgages, personal loans, debit cards, credit cards, and so forth.
Reverse REPO	:	The opposite side of a repo transaction.
Risk Adjusted Return on Capital (RAROC)	:	A measurement tool that enables management to allocate capital, and the related cost of capital, in respect of credit, market and operational risk by type of transaction, client and line of business. This facilitates the deployment of capital to business units that can provide the maximum shareholder value on the capital invested.
Risk Assessment	:	The identification of risk, the measurement of risk, and the process of prioritizing risks.
Risk Committee	:	A board level committee with responsibility for issues related to financial risk management.
Risk Factor	:	A random variable whose value will affect the value of a portfolio.
Risk Matrix	:	A form of Risk Measurement and Risk Prioritization in one step that uses risks on the horizontal axis and system components or audit steps on the left axis. Both axes are sorted to the left corner (High), creating a matrix with quadrants of High, Medium and Low groups of elements and risks.
Risk Reduction	:	Risk reduction is used in risk management to describe the application of appropriate techniques to reduce the likelihood of an occurrence, its consequences, or both. Along with risk avoidance, risk acceptance and risk transfer, risk reduction is one of the options for risk treatment.
SEC	:	Securities and Exchange Commission.
Secured Lending	:	Collateralized lending.
Securities Act of 1933	:	The US legislation to regulate the primary (underwriting) market for securities.
Securities Exchange Act of 1934	:	The US legislation to regulate the secondary market for securities.
Short Sale	:	Sale of a borrowed security.
Six Sigma	:	Six Sigma is a methodology that provides businesses with the tools to improve the capability of their business processes. This increase in performance and decrease in process variation leads to defect reduction and vast improvement in profits, employee morale and quality of product.
Special Electronic Fund Transfer (SEFT)	:	Established by some regulations for carrying out inter bank and intra-bank funds transfers within India, through Electronic Fund Transfer (EFT) centres connected by a network, and providing for settlement of payment obligations arising out of such funds transfers, between participating banks or institutions.

Supply Chain Management : Long-term partnerships among marketing channel members working together to reduce costs, waste, and unnecessary movement in the entire marketing channel in order to satisfy customers.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) : The industry owned co-operative supplying secure messaging services and interface software to approximately 7,000 financial institutions in around 200 countries.

Synthetic CDO : A CDO that creates credit exposures for investors primarily through CDSs. (Controlled Debt Structures).

System Development Life Cycle : Developing information systems by a process of investigation, analysis, design, implementation and maintenance.

TAC Bond : Targeted amortization class bond.

Tax Spread : A (usually negative) yield or interest rate spread due to some tax advantage.

T-Bills : Issued at a discount, T-bills are short-term debt securities issued or guaranteed by federal, provincial or other governments that mature at par. The return is calculated based on the difference between the price paid and the par value.

TCP/IP : Transmission Control Protocol/Internet Protocol. A *de facto* network architecture standard for many companies.

Technical Feasibility : Analyzing whether reliable hardware and software, capable of meeting the needs of a proposed system, can be acquired by the organization in time.

Theta : The Greek factor sensitivity measuring a portfolio's first order (linear) sensitivity to the passage of time.

Time Value of Money : Used informally to refer to the fact that the present value of future cash flows decreases with the amount of time until they are to be received.

Total Quality Management : Total Quality Management is a structured system for satisfying internal and external customers and suppliers by integrating the business environment, continuous improvement, and breakthroughs with development, improvement, and maintenance cycles while changing organizational culture.

Total Return Swap : A type of credit derivative.

Touch screen : Touch screens recognize human touch. Users can point to the select something on the screen

Transaction Processing System (TPS) : An information system that processes data arising from the occurrence of business transactions.

User Interface : User Interface is the component that humans use to communicate with computers.

Value-at-Risk	:	A category of market risk measures.
Vanilla Derivative	:	A derivative instrument that is simple or of a common form.
Vanilla Option	:	A simple put or call option.
Variance	:	A parameter describing the dispersion of a probability distribution.
Variance-Covariance VaR	:	Linear VaR.
Virtual Memory	:	The use of secondary storage as extension of the primary storage and giving the appearance of larger main memory than actually exists.
Vostro Account	:	A nostro account from the correspondent bank's point of view.
Wide Area Network (WAN)	:	A communications network that is spread out over a wide geographical area.
World Wide Web	:	The web is a system of Internet servers that support specially formatted documents with images, audio and video.
Zero Balance Accounts	:	A disbursement bank account on which cheques are written even though the balances in the accounts are maintained at zero. Debits are covered by a transfer of funds from a master account at the same bank.